

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-357365

(43)Date of publication of application : 26.12.2001

(51)Int.Cl. G06K 17/00

G06K 19/07

G06K 19/00

G09C 1/00

(21)Application number : 2000-180051 (71)Applicant : SONY CORP

(22)Date of filing : 15.06.2000 (72)Inventor : SHIRAI TAIZO

ISHIBASHI YOSHITO

ASANO TOMOYUKI

YOSHINO KENJI

OKA MAKOTO

TAKI RYUTA

(54) DATA STORAGE, DATA STORAGE METHOD AND RECORDING
MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To ensure security and also to simultaneously receive supply of plural types of services with a single IC card.

SOLUTION: The data which permit access to the service data on another type of service while a certain type of service is performed are registered on a service relation table when plural types of service are registered on an IC card. The service relation table includes a registered service ID field where the service IDs registered on the IC card are described and a permission information field where the permission information corresponding to each service ID is described. The

permission information describes a service ID that can be accessed when its corresponding service is performed and the information that shows the executable processing to the accessible service ID.

LEGAL STATUS [Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

JPO and NCIP are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.

2. **** shows the word which can not be translated.

3. In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] In the data storage with which an information processor is equipped and which performs transfer of said information processor and data An input/output control means against said information processor to control I/O of said data, The 1st storage control means which controls the data storage corresponding to two or more services, The 1st service ID corresponding to the 1st service of the services of said plurality When I/O of said data about said 1st service is controlled by said input/output control means, I/O of said data is permitted. Data storage characterized by having the 2nd storage control means which controls storage of the 2nd service ID corresponding to the 2nd service of the services of said plurality.

[Claim 2] Said 2nd storage control means is data storage according to claim 1 characterized by controlling further storage of the information about a limit of the

access privilege about said 2nd service.

[Claim 3] Said 2nd storage control means is data storage according to claim 1 characterized by controlling storage of two or more 2nd services ID of said when two or more said 2nd service ID exists to said 1st service ID, and controlling storage so that said 2nd service ID serves as a blank when one does not exist [said 2nd service ID] to said 1st service ID.

[Claim 4] In the data store method of the data storage with which an information processor is equipped and which performs transfer of said information processor and data The input/output control step to said information processor which controls I/O of said data, The 1st storage control step which controls the data storage corresponding to two or more services, The 1st service ID corresponding to the 1st service of the services of said plurality When I/O of said data about said 1st service is controlled by processing of said input/output control step, I/O of said data is permitted. The data store method characterized by including the 2nd storage control step which controls storage of the 2nd service ID corresponding to the 2nd service of the services of said plurality.

[Claim 5] The input/output control step which an information processor is equipped with, and is a program said information processor and for the data storage which performs transfer of data, and controls the I/O of said data to said information processor, The 1st storage control step which controls the data

storage corresponding to two or more services, The 1st service ID corresponding to the 1st service of the services of said plurality When I/O of said data about said 1st service is controlled by processing of said input/output control step, I/O of said data is permitted. The record medium with which the program which the computer characterized by including the 2nd storage control step which controls storage of the 2nd service ID corresponding to the 2nd service of the services of said plurality can read is recorded.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the data storage and the data store method which make it possible to perform in parallel transfer of the data about other services permitted beforehand, securing security, when the IC card and the reader writer are performing transfer of the data about predetermined service concerning data storage and a data store method.

[0002]

[Description of the Prior Art] Use of IC (Integrated circuit) card is increasing in a

cybermoney system and a security system. The IC card contains the memory which memorizes CPU (Central Processing Unit) which performs various processings, data required for processing, etc., and transmission and reception of data are performed by non-contact using the condition of having made the predetermined reader writer contacting electrically, or an electromagnetic wave. In addition, generally required power is supplied to the IC card transmit and receive data by non-contact between reader writers using an electromagnetic wave by the electromagnetic wave.

[0003] A common key system or a public key system is used for an IC card and authentication of a reader writer. The key used for decode is the same as the key used for encryption in a common key system. Since it is necessary to share a common key between a transmitting person and an addressee beforehand in order to use a common key cryptosystem, it is necessary to send the key used for encryption to a communications partner using safe means by which a channel is another (that is, the IC card and the reader writer must share the common key beforehand). Fundamentally, encryption is performed combining the "substitution" which transposes "the transposition (character transposition)" which replaces the sequence of an alphabetic character, and the alphabetic character according to a fixed regulation to another alphabetic character. Cryptographic algorithm and a key show in what kind of sequence it changes, or

which alphabetic character and which alphabetic character are replaced. In encryption, the number of alphabetic characters which the transposition code for changing the substitution cipher for shifting an alphabetic character and the sequence of an alphabetic character is fundamental code conversion, and is shifted serves as a key.

[0004] In a code system, the two keys an "encryption key" and a "decode key" are used for a public key system in a pair, the encryption key of them is exhibited, the publisher of a key manages a decode key and it is made secret. When transmitting data, correspondence is enciphered using an encryption key and it returns using a decode key in the side which received. Although it is not impossible to ask for a decode key from an encryption key since two keys are decided based on a certain mathematical relation, it is not realistic from the point of computational complexity.

[0005] Although it has the advantage of it not being necessary to distribute a decode key and having the authentication function of the message by the digital signature further since a public key cryptosystem should just have even the decode key which each user has separately in order distribution of an encryption key is easy and to decode a cipher, since it is not necessary to keep an encryption key secret compared with the conventional common key cryptosystem system, compared with a common key cryptosystem system,

the time amount concerning authentication processing becomes long.

[0006] A digital signature is an approach to show that it is sent by the addresser with the just message, and the alteration etc. is not performed on the way in an electronic mail, online dealings, etc. In the usual cipher communication link, although it enciphers with a public key, in the case of a RSA (Rivest, Shamir, Adleman) public key cryptosystem, it is "Enciphering with a decode key (private key)" with a digital signature conversely, for example. Moreover, in other cipher systems, to data to add a signature, the hash value was taken and it is enciphered with the private key.

[0007] A public key is used in order to verify this signature (that is, the role of an encryption key and a decode key is replaced). Since the public key is exhibited widely, anyone can inspect the justification of the signature easily. A public key can restore a cipher correctly, and if a meaningful sentence is obtained, it can be checked as he is a right addresser. Only the addresser of normal knows the private key (key which signed), and in order to create the digital signature which can be restored with a public key, it is because the private key used as the pair must be known. Moreover, when data are altered, since it becomes impossible to decode data correctly, they are applicable also to prevention and detection of an alteration. If verification of a signature is performed by comparing the value decoded using the public key with the hash value separately recalculated from

data, and is in agreement and it is not [it is judged that data are not altered and]
in agreement, it is judged that the alteration of data was performed.

[0008] Moreover, the organization of the 3rd person aiming at publishing the certificate for proving that he is the organization for which data issue-origin can set reliance is called certificate authority (CA (Certificate Authority)).

[0009]

[Problem(s) to be Solved by the Invention] Other services cannot be received while having received one service, when receiving two or more services conventionally using an IC card. In an IC card and a reader writer, it is because it is necessary to perform authentication processing in order to deliver and receive predetermined data and to secure the security to each data. However, when prepaid service and cybermoney service can be received for example, using the same reader writer as the same IC card, there is a demand of wanting to be filled up with cybermoney, performing liquidation processing about prepaid service.

[0010] It makes it possible to perform in parallel transfer of the data about other services permitted beforehand, securing security, when this invention is made in view of such a situation and transfer of the data about predetermined service is being performed.

[0011]

[Means for Solving the Problem] An input/output control means as opposed to an

information processor in the data storage of this invention and to control I/O of data, The 1st storage control means which controls the data storage corresponding to two or more services, The 1st service ID corresponding to the 1st service of two or more services When I/O of the data about the 1st service is controlled by the input/output control means, it is characterized by having the 2nd storage control means which controls storage of the 2nd service ID corresponding to the 2nd service of two or more services to which I/O of data is permitted.

[0012] The 2nd storage control means can be made to control storage of the information about a limit of the access privilege about the 2nd service.

[0013] When two or more 2nd service ID exists to the 1st service ID, storage of two or more 2nd services ID is made to control, and the 2nd storage control means can be made to control storage so that the 2nd service ID serves as a blank when one does not exist [the 2nd service ID] to the 1st service ID.

[0014] The input/output control step by which the data store method of this invention controls the I/O of data to an information processor, The 1st storage control step which controls the data storage corresponding to two or more services, The 1st service ID corresponding to the 1st service of two or more services I/O of data is permitted when I/O of the data about the 1st service is controlled by processing of an input/output control step. It is characterized by

including the 2nd storage control step which controls storage of the 2nd service ID corresponding to the 2nd service of two or more services.

[0015] The program currently recorded on the record medium of this invention

The input/output control step to an information processor which controls I/O of data, The 1st storage control step which controls the data storage corresponding to two or more services, The 1st service ID corresponding to the 1st service of two or more services I/O of data is permitted when I/O of the data about the 1st service is controlled by processing of an input/output control step. It is characterized by including the 2nd storage control step which controls storage of the 2nd service ID corresponding to the 2nd service of two or more services.

[0016] In the program currently recorded on the data storage, data store method, and record medium of this invention The 1st service ID corresponding to [I/O of the data to an information processor is controlled, and the data storage corresponding to two or more services is controlled, and] the 1st service of two or more services When I/O of the data about the 1st service is controlled by processing of an input/output control step, storage of the 2nd service ID corresponding to the 2nd service of two or more services to which I/O of data is permitted is controlled.

[0017]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention

is explained with reference to drawing.

[0018] The relation between an IC card and a reader writer is shown in drawing 1. IC card 1 can be dealt with authentication service of both authentication by the common key system, and the authentication by the public key system (about each authentication approach, it mentions later). The reader writer 2-1 corresponding to a non-contact type common key communicates by IC card 1 and non-contact, and attests with a common key system. The reader writer 2-2 corresponding to a non-contact type public key communicates by IC card 1 and non-contact, and attests with a public key system. The reader writer 2-3 corresponding to a contact process public key communicates by contacting, and communicates with a public key system.

[0019] For example, the information which offers service of the prepaid card which can perform payment of a commuter pass or a fare is included in IC card 1. To the case where the ticket gate of a station is used using IC card 1, and IC card 1 The function as an ID card is included and the non-contact communication link with a common key is performed using the reader writer 2-1 corresponding to a non-contact type common key in the processing asked for the short processing times in the case of attesting entrance authorization using IC card 1 etc.

[0020] For example, the information which offers service of cybermoney is

included in IC card 1, when processing liquidation of the goods which the user purchased at the store etc., authentication is performed by the public key system and authentication processing takes time amount. For this reason, when not caring especially about the processing time, in order to communicate by non-contact and to shorten the processing time using the reader writer 2-2 corresponding to a non-contact type public key, the reader writer 2-3 corresponding to a contact process public key is used, and it may be made to communicate by contacting.

[0021] Although the reader writer 2-1 thru/or the reader writer 2-3 corresponding to a contact process public key corresponding to a non-contact type common key is explained as a reader writer according to individual, it is one reader writer and you may enable it to use two or more correspondence procedures and two or more authentication approaches in drawing 1 if needed.

[0022] Next, a card publisher, a service provider, and a card holder are explained using drawing 2 .

[0023] The card publisher 11 approves providing a service provider 12 with the service using IC card 1 to the card holder 13 who holds IC card 1, and publishes IC card 1 to the card holder 13 who wished issue of IC card 1.

[0024] From the card publisher 11, the service provider 12 which received license of service registers the data (Service Individual Info later mentioned

using drawing 6) corresponding to the service with which he provides the card holder 13 into the reader writer 2-11 for service registration which the card publisher 11 has. You may make it register with the reader writer 2-11 for service registration, and an operator may be made to register manually through the Internet etc. about this registration from the personal computer which a service provider 12 has and which is not illustrated, for example.

[0025] The card holder 13 can make it register into IC card 1 published by the card publisher 11 using the reader writer 2-11 for service registration to give [to wish one's service]. About the reader writer 2-11 for service registration, and service registration processing of IC card 1, it mentions later using drawing 29 and drawing 30 .

[0026] And the card holder 13 can make service delete from its own IC card 1 using the reader writer 2-11 for service registration which the card publisher 11 manages, or the general reader writer 2-12 which a service provider 12 manages to delete service registered into its own IC card 1. About the service deletion of IC card 1 and the reader writer 2-11 for service registration, it mentions [deletion / of drawing 31 and drawing 32 , IC card 1, and the general reader writer 2-12 / service] later using drawing 33 and drawing 34 .

[0027] Moreover, cybermoney service and prepaid service are registered into IC card 1, and the card holder 13 is in the situation that each value information is

recorded on the information about each service of IC card 1. When you want to transpose a part of worth of cybermoney to prepaid value, Intermodule communication can be performed using the reader writer 2-13 for intermodule communications which a service provider 12 manages between the public key module later mentioned using drawing 13 of its own IC card 1, and a common key module. The reader writer 2-13 for intermodule communications is made as [correspond / to a common key system and two methods of a public key system]. About processing with IC card 1 and the reader writer 2-13 for intermodule communications, it mentions later using drawing 48 thru/or drawing 51 .

[0028] Furthermore, the card holder 13 can make the authentication key registered into its own IC card 1 upgrade using the general reader writer 2-12 which a service provider 12 manages, or the reader writer 2-14 for version up to update the invalidated authentication key (version up). About key version up processing with IC card 1 and the reader writer 2-14 for version up, it mentions [processing / with IC card 1 and the general reader writer 2-12 / key version up] later using drawing 45 thru/or 47 using drawing 43 and 44.

[0029] Drawing 3 is the block diagram showing the configuration of IC card 1.

[0030] IC card 1 consists of the communications department 21 which performs the communication link with the reader writer 2 (these shall be named

generically and the reader writer 2 shall be called about the case where there is no need of distinguishing the reader writer 2-1 thru/or 2-3 or the reader writer 2-11 thru/or especially 2-14), and the IC card processing section 22 which performs data processing.

[0031] The communications department 21 has the coil for communicating with the reader writer 2-1 corresponding to a non-contact type common key, or the reader writer 2-2 corresponding to a non-contact type public key using an electromagnetic wave, when corresponding IC card 1 is the reader writer 2-1 corresponding to the non-contact type common key explained using drawing 1 , or the reader writer 2-2 corresponding to a non-contact type public key. moreover, IC card 1 the communications department 21 only not only in the reader writer 2-1 corresponding to the non-contact type common key explained using drawing 1 , and the reader writer 2-2 corresponding to a non-contact type public key When the communication link with the reader writer 2-3 corresponding to a contact process public key is also supported, the reader writer 2-1 corresponding to a non-contact type common key, or the reader writer 2-2 corresponding to a non-contact type public key, It has the coil for communicating using an electromagnetic wave, and the contact terminal for communicating with the reader writer 2-3 corresponding to a contact process public key.

[0032] The communications department 21 receives the data transmitted from

the reader writer 2, and the received data When becoming irregular using ASK (Amplitude Shift Keying) or BPSK (Binary Phase Shift Keying), for example, by predetermined processing While restoring to the received data and supplying the control section 31 of the IC card processing section 22, the data generated by processing of the IC card processing section 22 are supplied from a control section 31, and it becomes irregular using ASK or BPSK, and transmits to the reader writer 2.

[0033] The IC card processing section 22 consists of a control section 31, memory 32, and the cipher-processing section 33. According to the data supplied from the communications department 21, a control section 31 controls the cipher-processing section 33, cipher processing required for authentication processing with the reader writer 2 etc. is performed, or it reads the data currently recorded on memory 32 if needed, and transmits to the reader writer 2 through the communications department 21.

[0034] Memory 32 consists of a memory area 44 where CA_Pub which is Card ID, the authentication key Kreg for service registration, and the public key of a certificate authority is recorded, Service Relation Table (SRT)⁴⁵ later mentioned using drawing 8 , and Service Registration Area (SRA)⁴⁶ later mentioned using drawing 6 .

[0035] The cipher-processing section 33 consists of the public key processing

section 41, the common key processing section 42, and the other cipher-processing sections 43. The detail about the processing which the public key processing section 41 thru/or the other cipher-processing sections 43 perform is later mentioned using drawing 5 .

[0036] Next, drawing 4 is the block diagram showing a different configuration from drawing 3 of IC card 1. In addition, in IC card 1 of drawing 4 , the same sign is given to the case in drawing 3 , and the corresponding part, and the explanation is omitted suitably (following, the same).

[0037] IC card 1 consists of the public key service processing sections 54 which perform processing of the data obtained by processing of the communications department 51 which performs the communication link with the reader writer 2 about common key service, the common key service processing section 52 which performs processing of the data obtained by processing of the communications department 51, the communications department 53 which performs the communication link with the reader writer 2 about public key service, and the communications department 53.

[0038] The communications department 51 has the coil for communicating with the reader writer 2-1 corresponding to a non-contact type common key. When the data transmitted from IC card 1 are modulated like the communications department 21 using ASK or BPSK, by predetermined processing While

restoring to the received data and supplying the control section 61 of the common key service processing section 52, the data generated by processing of the common key service processing section 52 are supplied from a control section 61, and it becomes irregular using ASK or BPSK, and transmits to the reader writer 2.

[0039] The common key service processing section 52 consists of a control section 61, memory 62, and the cipher-processing section 63. According to the data supplied from the communications department 51, a control section 61 controls the cipher-processing section 63, processing required for authentication processing with IC card 1 etc. is performed, or it reads the data currently recorded on memory 62 if needed, and transmits to the reader writer 2 through the communications department 51.

[0040] Memory 62 consists of a memory area 44, and SRT45 and SRA46 like the memory 32 explained using drawing 3 . Share private key K_{common} used by the authentication key K_{reg} and intermodule communication Card ID and for service registration is recorded on the memory area 44.

[0041] The cipher-processing section 63 consists of the common key processing section 42 and the other cipher-processing sections 43. That is, in the common key service processing section 52, in order not to process the service about a public key, the cipher-processing section 63 is not equipped with the public key

processing section 41 explained using drawing 3 .

[0042] The communications department 53 has the coil or contact terminal for communicating with the reader writer 2-2 corresponding to a non-contact type public key, or the reader writer 2-3 corresponding to a contact process public key. When the data with which the communications department 53 is also transmitted from IC card 1 are modulated using ASK or BPSK, like the communications department 21 by predetermined processing While restoring to the received data and supplying the control section 61 of the public key service processing section 54, the data generated by processing of the public key service processing section 54 are supplied from a control section 61, and it becomes irregular using ASK or BPSK, and transmits to the reader writer 2.

[0043] The public key service processing section 54 consists of a control section 61, memory 62, and the cipher-processing section 33. That is, except that it has the cipher-processing section 33 explained using drawing 3 instead of the cipher-processing section 63, it is the same configuration fundamentally with the common key service processing section.

[0044] Next, the public key processing section 41 thru/or the other cipher-processing sections 43 are explained using drawing 5 .

[0045] As shown in drawing 5 (A), the public key processing section 41 is equipped with RSA signature generation / verification section 71 which performs

generation and verification of a signature using a RSA (Rivest, Shamir, Adleman) public key cryptosystem, and DSA signature generation / verification section 72 which performs generation and verification of a signature using a DSA (Digital Signature Algorithm) method.

[0046] In RSA signature generation / verification section 71, two keys perform encryption and decode. In a RSA cryptosystem, two keys are decided as follows, for example.

[0047] Some two big prime factors p and q are chosen, and the product $n=pq$ is calculated. And x $(p-1) (q-1)$ and the relatively prime integer e are chosen below by x $(p-1) (q-1)$, and the integer d with which the following formula (1) is filled is searched for.

$$Exd = 1 \text{ mod } \dots (x (p-1) (q-1)) \quad (1)$$

Then (e, n) , a public key and d become a private key.

[0048] When enciphering Sentence M and generating the encryption data C , the following formula (2) is used.

$$C=M^e \text{ mod } n \dots \quad (2)$$

Moreover, when decoding the encryption data C , the following formula (3) is used.

$$M=C^d \text{ mod } n \dots \quad (3)$$

[0049] DSA signature generation / verification section 72 is equipped with the

random-number generation section which is not illustrated. DSA is a digital signature algorithm which improves the ElGamal signature which used the difficulty of DLP (Discrete Logarithm Problem; dispersion a logarithm problem) as the base, shortens the die length of a signature to 160bitx2, and employs generation of a signature key etc. by the specific approach. It is premised on using SHA-1 (Secure Hash Algorithm-1) for a Hash Function (data compression function) in signature generation. The DSA method was developed as a criterion of electronic signature by NIST (U.S. Department of Commerce standard technical station: National Institute of Standards and Technology) which is the U.S. Government engine, and was set to U.S. Federal Information Processing Standard (Federal Information Processing Standard) FIPS PUB 186.

[0050] Moreover, as shown in drawing 5 (B), the common key processing section 42 is equipped with the DES processing section 73 which performs authentication processing by the DES (Data Encryption Standard) common key cryptosystem system, RC5 processing section 74 which performs authentication processing by RC5 (Rivest Cipher5) method, and the AES processing section 75 which performs authentication processing by the AES (Advanced Encryption Standard) method.

[0051] A DES common key cryptosystem system is a common key cryptosystem system which was enacted in NIST in 1977 and standardized by

American National Standards Institute (ANSI:American National Standards Institute) in 1981. The authentication algorithm of the key of a DES common key cryptosystem system is exhibited, and has spread widely as a representative of a common key cryptosystem system.

[0052] A DES common key cryptosystem system is a code system which divides data per 64 bits and performs encryption and decode processing. In a DES algorithm, encryption and decode are making the symmetry, and if the received cipher is changed once again using the same key, they can restore the original text. Moreover, in the DES common key cryptosystem system, the combination logic of easy bit-position transposition and an XOR operation is repeated 16 times. Since processing is successive, if there are no feedback and conditional-judgment part of data internally, and it pipelines, it can process at a high speed. It is the algorithm decided on the assumption that it LSI-ized from the first, and many DES chips are also made.

[0053] In RC5, it is the common key encryption system of RSA Data Security and RC series which Massachusetts Institute of Technology developed, and was proposed in 1995. RC5 is a block cipher system which has a variable-length block size, variable-length key size, and the round of the count of variable length (Data dependent rotations (data dependence bit rotation) algorithm which changes the amount of bit rotation with former data or a key). As the block size, it

is possible to take 32 or 64,128 bits, the number of rounds is 0 to 255, and key size is adjustable to 0 to 2048 bits. It is possible for the algorithm of RC5 to be exhibited and to receive as RFC2040.

[0054] Moreover, an AES method is a next-generation standard cipher system of the U.S. Government with which selection is performed by NIST. It is that DES used as a current standard code was enacted, and the dependability is falling every year with high-performance-izing of a computer in recent years, and development of the code theory. Then, NIST sought the cipher system which serves as an AES candidate from the whole world as a code criterion of the next generation replaced with DES. The method of 15 which gathered from all over the world is undergoing the examination, and is due to be determined by the beginning of the 21st century.

[0055] And to a message, it is making an irreversible Hash Function act, and the other cipher-processing sections 43 perform cipher processing except the public key processing section 41 or the common key processing section 42 of creating a digital signature processing by creating a "message digest" and enciphering a message digest with a signature key, when using a digital signature. In the other cipher-processing sections 43, as shown in drawing 5 (C) For example, [whether it has the SHA-1 processing section 76 which processes Hash Function SHA-1 used for signature generation and signature verification, and the

intrinsic random-number generation section 77 which generates the intrinsic random number used with a mutual recognition protocol, and] Or as shown in drawing 5 (D) The MD5 processing section 78 which processes Hash Function MD5 used for signature generation and signature verification, and the pseudo-random number (artificial random number which has the random possible digit string in the range of the figure of the existing limited digit count) used with a mutual recognition protocol It has the pseudo-random-number generation section 79 to generate.

[0056] In a digital signature, although that processing speed is slow poses a problem in order to use a public key cryptosystem, the time amount concerning digital signature creation is reduced by creating a message digest. Furthermore, since the Hash Function has the property of reacting greatly to the alteration of data, in case it verifies a digital signature, it can check easily whether the message body is altered by comparing the message digest which decoded and took out the digital signature with the verification key with the message digest which the Hash Function was made to act on the sent message body, and was created.

[0057] SHA-1 is an one-way hash function which generates the hash value of 160 bits from the message of the die length of arbitration. Like DSA, it is what NIST developed and is FIPS PUB180 by NIST. It was set. Standard draft

proposal (N544) is what was fundamentally based on FIPS PUB 180.

[0058] And MD5 is one of the message digest function algorithms currently generally used widely, and is defined by RFC1321. The algorithm is decided so that MD5 can be efficiently calculated on a 32-bit computer. There is also another similar algorithm [say / MD4 or MD2].

[0059] Next, the information stored in SRA46 of IC card 1 explained using drawing 3 and drawing 4 is explained using drawing 6 .

[0060] SRA46 is a memory area for recording the information (information registered using the reader writer 2-11 for service registration explained using drawing 2) for receiving those services of two or more, in order that the user who holds IC card 1 may enable it to receive two or more services using the general reader writer 2-12 explained using drawing 2 .

[0061] Namely, Service Individual Info1 thru/or N which is the information on the service registered into the IC card 1 is registered into SRA46. In each Service Individual Info Were beforehand set for every service ID for identifying the class of service, and service. One or two or more key information for authentication (in Service Individual Info k in drawing 6) The certificate to an authentication key etc. is registered if needed with authentication key Kake_vup for upgrading the service data used in order to receive 1 thru/or the key information for n authentications on n, and service, and key information.

[0062] The authentication key Kake for discernment (certificate [as opposed to an authentication key according to the need]) used in order to identify the level of for example, the authentication key ID and a key and a version, an authentication method, and two or more authentication keys is contained in the key information for authentication. Moreover, in addition to user ID, when Service Individual Info k is for example, cybermoney service, and Service Individual Info k, such as balance information, the accumulation point, etc. of cybermoney, is for example, automatic wicket services, effective section information etc. is stored in service data.

[0063] Next, the key information for authentication registered into Service Individual Info of drawing 6 is explained using drawing 7 .

[0064] In drawing 7 (A), certificate data are registered the version of the authentication key ID and a key, an authentication method, the authentication key Kake for discernment, and if needed corresponding to each of field No.1 and field No.2. About authentication key discernment processing in case the key information for authentication is registered like drawing 7 (A), it mentions later using drawing 20 thru/or drawing 24 .

[0065] In drawing 7 (B), certificate data are registered the level of the authentication key ID and a key, the version of a key, an authentication method, the authentication key Kake for discernment, and if needed corresponding to

each of field No.1 thru/or field No.7. About authentication key discernment processing in case the key information for authentication containing the level of a key is registered like drawing 7 (B), it mentions later using drawing 27 and drawing 28 .

[0066] Next, the information stored in SRT45 of IC card 1 explained using drawing 3 and drawing 4 is explained using drawing 8 .

[0067] When two or more services are registered into ID card 1 by SRT45, the data for permitting access to the service data of another service are registered into it, offering a certain service. SRT45 consists of a registration service ID field (drawing 8 is indicated as services IDA and J) the service ID registered into IC card 1 is indicated to be, and permission information field where the permission information corresponding to each service ID is indicated.

[0068] The services ID of the service registered are altogether enumerated by the registration service ID field of permission information. And when corresponding service is performed, the information which shows what kind of processing [the service ID which can access the service indicated by the registration service ID field, and] it permits are performed is indicated in permission information field. For example, when read-out and writing are permitted, "rw" is indicated as permission information, when only read-out is permitted, "ro" is indicated as permission information, and when version up of a

key is permitted, "vup" is indicated as permission information. Although "rw" and "ro" are not permitted to the same service ID, a permission is granted to the same service ID and "rw", "vup", and "ro" and "vup" can be enumerated to permission information field.

[0069] namely, when the permission information shown in drawing 8 is registered into SRT45, during activation of the service Service ID is indicated to be by C It is also under [activation / of the service with which read, and writing is permitted to the service Service ID is indicated to be by B, and Service ID is further indicated to be by D] also setting. As opposed to the service Service ID is indicated to be by D during activation of the service with which read-out to the service Service ID is indicated to be by B is permitted, and Service ID is indicated to be by E Read-out, writing, and version up of a key are permitted. The following, the service Service ID is indicated to be by E, the service Service ID is indicated to be by F, and the service Service ID is indicated to be by G -- or Also in the service Service ID is indicated to be by I, the processing corresponding to permission information is permitted during activation of the processing corresponding to other services ID based on the information indicated in corresponding permission information field.

[0070] Registration of such permission information is performed when registering the service corresponding to IC card 1. Namely, a user receives IC

card 1 which he holds using the reader writer 2-11 for service registration. If the service Service ID is indicated to be by G is already registered and the service Service ID is indicated to be by H is not registered when registering the service Service ID is indicated to be by F for example Only the permission information corresponding to the service Service ID is indicated to be by G can be registered into the permission information field corresponding to F of a registration service ID field. And after a user registers into ID card 1 the service Service ID is indicated to be by H, the permission information on service over the service Service ID is indicated to be by F by which Service ID is shown by H can be registered by updating the service Service ID is indicated to be by F.

[0071] Next, drawing 9 is the block diagram showing the configuration of the reader writer 2.

[0072] The reader writer 2 consists of the communications department 91 which performs the communication link with IC card 1, and the reader writer processing section 92 which performs data processing.

[0073] The communications department 91 has structure equipped with the contact terminal for communicating by the coil for having only a coil for namely, communicating using an electromagnetic wave by whether the reader writer 2 has adopted which communication mode of the non-contact type explained using drawing 1 , and a contact process, or communicating by the

correspondence procedure with IC card 1, using an electromagnetic wave, and the contact process.

[0074] When the communications department 91 receives the data transmitted from IC card 1 and the received data are modulated using ASK or BPSK, by predetermined processing While restoring to the received data and supplying the control section 101 of the reader writer processing section 92, the data generated by processing of the reader writer processing section 92 are supplied from a control section 101, and it becomes irregular using ASK or BPSK, and transmits to IC card 1.

[0075] The reader writer processing section 92 consists of a control section 101, the cipher-processing section 102, memory 103, the communications department 104, a display 105, and the input section 106. A control section 101 controls the cipher-processing section 102 according to the data supplied from the communications department 91, and the data currently recorded on memory 103 are read if needed in performing cipher processing required for authentication processing with IC card 1 etc. ****. The signal corresponding to the various actuation which the user inputted, using the input section 106 in transmitting to IC card 1 ****, and a network are minded through the communications department 91. The input of the control signal inputted into the communications department 104 is received, processing is performed according

to these signals, and the result is displayed on a display 105.

[0076] moreover, transfer of the magnetic disk 115 with which the drive 114 is also connected to the communications department 104, and drive 114 is equipped, an optical disk 116, a magneto-optic disk 117 semiconductor memory 118, etc. and data -- a line -- things are made.

[0077] Since it has the same configuration as the cipher-processing section 33 explained using drawing 3 , the cipher-processing section 102 omits the explanation.

[0078] The information for performing processing of IC card 1 and predetermined is memorized by memory 103. The information differs by the thing corresponding to any of the reader writer 2-11 for service registration explained using drawing 2 thru/or the reader writer 2-14 for version up the reader writer 2 is. The data memorized by the memory 103 of the reader writer 2-11 for service registration thru/or the reader writer 2-14 for version up are explained using drawing 10 thru/or drawing 14 .

[0079] The authentication key Kreg used for the memory 103 of the reader writer 2-11 for service registration shown in drawing 10 when registering or deleting data to SRA46 of the memory 32 of IC card 1 is memorized (the certificate of an authentication key is also memorized if needed), and Service Individual Info1 thru/or n corresponding to the various services for registering with IC card 1 is

memorized.

[0080] The service ID corresponding to the service which can be processed by this general reader writer 2-12, the authentication key list corresponding to it, and key lapse information are memorized by the memory 103 of the general reader writer 2-12 shown in drawing 11 . Moreover, when making the general reader writer 2-12 enable service of key version up, the information on the key of an upgrade product etc. is also united and memorized by the memory 103 of the general reader writer 2-12 at it.

[0081] The service ID corresponding to the service which can be processed by this reader writer 2-13 for intermodule communications, the authentication key list corresponding to it, and key lapse information as well as the information memorized by the memory 103 of the general reader writer 2-12 are memorized by the memory 103 of the reader writer 2-13 for intermodule communications shown in drawing 12 . As indicated in drawing 13 as intermodule communication, to the reader writer 2-13 for intermodule communications currently made as [correspond / to two methods of a common key system and a public key system] The public key module 121 (for example, it corresponds to the communications department 53 of IC card 1 which explained using drawing 4 , and the public key service processing section 54), It equips with IC card 1 which has the common key module 122 (for example, it corresponds to the

communications department 51 of IC card 1 explained using drawing 4 , and the common key service processing section 52). It is performing the communication link of the data of the public key module 121 and the common key module 122 through the reader writer 2-13 for intermodule communications. The detail of the processing about intermodule communication is later mentioned using drawing 48 thru/or drawing 51 .

[0082] And the list of authentication key Kake_vup for version up corresponding to Service ID and its service ID and the authentication keys Kake for upgrading the authentication key of the service registered into IC card 1 with which it was equipped to the memory 103 of the reader writer 2-14 for version up shown in drawing 14 is memorized.

[0083] When IC card 1 and the reader writer 2 communicate, in order for the reader writer 2 to carry out mutual recognition to IC card 1 first except for processing used as some exceptions, it is necessary to identify the service which communicates mutually and to identify the authentication key of the service mutually. With reference to the flow chart of drawing 15 , mutual recognition processing of IC card 1 and the reader writer 2 is explained.

[0084] First, in step S1, the reader writer 2 performs service discernment processing of the reader writer 2 later mentioned using drawing 16 and drawing 18 by communicating with IC card 1, and delivering and receiving required data

if needed. And in step S2, IC card 1 performs service discernment processing of IC card 1 later mentioned using drawing 17 and drawing 19 by communicating with the reader writer 2, and delivering and receiving required data if needed.

[0085] And by communicating with IC card 1, and delivering and receiving required data if needed, when service discernment processing of the reader writer 2 of step S1 and service discernment processing of IC card 1 of step S2 terminate normally, in step S3, the reader writer 2 performs authentication key discernment processing of the reader writer 2 later mentioned using drawing 20 , drawing 22 , and drawing 27 . And in step S4, IC card 1 performs authentication key discernment processing of IC card 1 later mentioned using drawing 21 , drawing 23 , and drawing 28 by communicating with the reader writer 2, and delivering and receiving required data if needed.

[0086] Next, by a user's inputting desired service in the reader writer 2 corresponding to two or more services, and judging it whether activation of the service is possible to be IC card 1 corresponding to two or more services with reference to the flow chart of drawing 16 , explains service discernment processing of the reader writer 2 performed in step S1 of drawing 15 .

[0087] To IC card 1, through the communications department 91, the control section 101 of the reader writer 2 transmits an IC card detection command, and judges whether the ACK signal (signal which IC card 1 transmitted in step S22 of

drawing 17 mentioned later) was received from IC card 1 in step S12 in step S11.

In step S12, when it is judged that the ACK signal is not received, processing of step S12 is repeated until it is judged that the ACK signal was received.

[0088] When it is judged in step S12 that the ACK signal was received, it sets to step S13 (namely, when the reader writer 2 is equipped with IC card 1). A control section 101 According to the signal which shows the actuation which the user inputted using the input section 106, the service ID corresponding to giving [which a user wishes] is transmitted to IC card 1 through the communications department 91 based on the service for which it opted beforehand.

[0089] In step S14, a control section 101 receives the signal (signal which IC card 1 transmitted in step S25 or step S26 of drawing 17 mentioned later) transmitted from IC card 1. In step S15, the data which the control section 101 received in step S14 judge whether it is an ACK signal. In step S15, when the received signal is judged not to be an ACK signal (that is, for it to be a NACK signal), in step S16, a control section 101 outputs and displays the data corresponding to an error message on a display 105, and ends processing (that is, processing does not progress to step S3 of drawing 15). In step S15, when the received signal is judged to be an ACK signal, processing progresses to step S3 of drawing 15 .

[0090] Next, with reference to the flow chart of drawing 17 , the service

discernment processing of IC card 1 performed in parallel to service discernment processing of the reader writer 2 explained using drawing 16 is explained in step S2 of drawing 15 . In addition, although here explains as that to which processing is performed in IC card 1 explained using drawing 3 , when processing is performed with IC card 1 explained using drawing 4 , same processing is performed fundamentally.

[0091] In step S21, in step S11 of drawing 16 , the control section 31 of IC card 1 receives the IC card detection command which the reader writer 2 transmitted through the communications department 21, and transmits an ACK signal to the reader writer 2 in step S22.

[0092] A control section 31 is set to step S13 of drawing 16 in step S23. The service ID which received the service ID which the reader writer 2 transmitted through the communications department 21, and was received in step S24 The module with which IC card 1 corresponds (although it corresponds to the memory 32 of the IC card processing section 22 here since the processing in IC card 1 explained using drawing 3 is explained) In the case of IC card 1 explained using drawing 4, with the method with which the reader writer 2 corresponds For example, the memory 62 of the common key service processing section 52 Or it judges whether the service ID received in whether it is ID registered while corresponding to the memory 62 of the public key service processing section,

and step S23 is registered into SRA46 explained using drawing 6 .

[0093] In step S24, when the received service ID is judged to be registered into a module, in step S25, a control section 31 transmits an ACK signal to the reader writer 2 through the communications department 21, and processing progresses to step S4 of drawing 15 . In step S24, when the received service ID is judged not to be registered into a module, in step S26, a control section 31 transmits a NACK signal to the reader writer 2 through the communications department 21, and processing is ended (that is, it does not progress to step S4 of drawing 15).

[0094] Next, with reference to the flow chart of drawing 18 , it sets to IC card 1 corresponding to two or more services, and the reader writer 2 corresponding to two or more services. By extracting corresponding IC card 1 and the service which can perform the reader writer 2, making it display on the display 105 of the reader writer 2, and making the service for which a user asks choose from those services Service discernment processing of the reader writer 2 performed in step S1 of drawing 15 in the case of performing service discernment is explained.

[0095] The control section 101 of the reader writer 2 judges whether the service ID list which IC card 1 transmitted was received in step S31 in step S52 of drawing 19 which transmits to IC card 1 through the communications department 91, and mentions a service ID list transmitting command later in step S32. In step S32, when it is judged that the service ID list is not received, processing of

step S32 is repeated until it is judged that the service ID list was received.

[0096] In step S32, when it is judged that the service ID list was received, in a control section 101, in step S33, the service ID indicated by the received service ID list judges whether the service which the reader writer 2 supports is included (that is, is the service ID memorized by the memory 103 of the reader writer 2 included or not?).

[0097] In step S33, when it is judged that the service corresponding to a reader writer is included in the received service ID list, in step S34, a control section 101 judges whether the correspondence service included in the service ID list is plurality. In step S34, when correspondence service is judged not to be plurality (that is, for it to be only one), processing progresses to step S37.

[0098] In step S34, when correspondence service is judged to be plurality, in step S35, a control section 101 generates the data for displaying two or more correspondence services on a display 105, is made to output and display them on a display 105, and receives the input of giving [which a user wishes] from the input section 106 in step S36. Or priority information is included in each service and the highest service of a priority may be made to be chosen from from automatically among two or more correspondence services.

[0099] In step S37, when it is judged in step S34 that correspondence service is only one, a control section 101 When correspondence service is judged to be

plurality in step S34, the service ID corresponding to the service In step S36, the service ID corresponding to giving [which the user inputted using the input section 106 / to wish one's service] is transmitted to IC card 1 through the communications department 91, and processing progresses to step S3 of drawing 15 .

[0100] When it is judged that the service corresponding to a reader writer is not included in the received service ID list in step S33, a control section 101 In step S38, through the communications department 91, a NACK signal is transmitted to IC card 1, the same processing as step S16 of drawing 16 is made in step S39, and processing is ended (that is, processing does not progress to step S3 of drawing 15).

[0101] Next, with reference to the flow chart of drawing 19 , the service discernment processing of IC card 1 performed in parallel to service discernment processing of the reader writer 2 explained using drawing 18 is explained in step S2 of drawing 15 . In addition, although here explains as that to which processing is performed in IC card 1 explained using drawing 3 , when processing is performed with IC card 1 explained using drawing 4 , same processing is performed fundamentally.

[0102] In step S51, the reader writer 2 receives the service ID transmitting command transmitted in step S31 of drawing 18 through the communications

department 21, and the control section 31 of IC card 1 generates the service ID list (namely, list of services ID registered into SRA46 of memory 32) with which he corresponds in step S52, and transmits to the reader writer 2 through the communications department 21.

[0103] A control section 31 receives the data which the reader writer 2 transmitted to IC card 1 in step S37 or step S38 of drawing 18 through the communications department 21 in step S53, and the data received from the reader writer 2 judge whether it is a NACK signal in step S54. In step S54, when the received signal is judged to be a NACK signal, processing is ended (that is, processing does not progress to step S4 of drawing 15). (namely, when the received data are the signal which the reader writer 2 transmitted to IC card 1 in step S38 of drawing 18)

[0104] In step S54, when it is judged that the data received from the reader writer 2 are not a NACK signal, in step S55, a control section 31 judges whether the service ID received from the reader writer 2 is registered into SRA46 of its own memory 32 (namely, when the received data are the service ID which the reader writer 2 transmitted to IC card 1 in step S37 of drawing 18).

[0105] In step S55, when it is judged that Service ID is not registered, processing is ended (that is, processing does not progress to step S4 of drawing 15). In step S55, when it is judged that Service ID is registered, processing progresses

to step S4 of drawing 15 .

[0106] Next, when authentication key discernment is performed with reference to the flow chart of drawing 20 using the key information for authentication that it explained using drawing 7 (A), authentication key discernment processing of the reader writer 2 performed in step S3 of drawing 15 is explained.

[0107] It is the service ID corresponding to the service from which the control section 101 of the reader writer 2 was discriminated in step S61 by service discernment processing of step S1 of drawing 15 , and step S2 (here). Read from memory 103, transmit to IC card 1 through the communications department 91, and the authentication key ID corresponding to one of the authentication keys which belong for making corresponding service ID into ID_S is set to step S62. The data which IC card 1 transmits are received in step S73 or step S75 of drawing 21 mentioned later.

[0108] In step S63, the data which the control section 101 received from IC card 1 in step S62 judge whether it is an ACK signal. When it is judged in step S63 that the ACK signal was received, it sets to step S64. A control section 101 The cipher-processing section 33 is controlled and it sets to step S61. The inside of the public key processing section 111 of the cipher-processing section 102, or the common key processing section 112, By choosing and controlling the processing section which performs authentication processing using the

authentication key corresponding to the authentication key ID transmitted to IC card 1 Processing is ended, after starting mutual recognition processing with IC card 1, and key share processing, sharing IC card 1 and the session key Kses and completing mutual recognition processing.

[0109] In step S63, when it is judged that the ACK signal is not received, in step S65, the same processing as step S16 of drawing 16 is made, and processing is ended (namely, when it is judged that the NACK signal was received).

[0110] Next, with reference to the flow chart of drawing 21 , the authentication key discernment processing of IC card 1 performed in parallel to authentication key discernment processing of the reader writer 2 of drawing 20 is explained in step S4 of drawing 15 . In addition, although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4 , same processing is performed fundamentally.

[0111] The control section 31 of IC card 1 judges whether the authentication key ID which received the authentication key ID which the reader writer 2 transmitted through the communications department 21, and was received in step S71 in step S72 is registered into the field to which the data about ID_S of SRA46 of memory 32 are memorized in step S61 of drawing 20 in step S71.

[0112] When it is judged in step S72 that the authentication key ID is registered,

a control section 31 In step S73, through the communications department 21, transmit an ACK signal to the reader writer 2, and it sets to step S74. By choosing and controlling the direction which performs authentication processing with the authentication key specified as the reader writer 2 among the public key processing section 41 of the cipher-processing section 33, or the common key processing section 42 Mutual recognition processing is performed, the reader writer 2 and the session key Kses are shared, and processing is ended after termination of mutual recognition processing. In step S72, when it is judged that the authentication key ID is not registered, in step S75, a control section 31 transmits a NACK signal to the reader writer 2 through the communications department 21, and processing is ended.

[0113] In the processing explained using drawing 20 and drawing 21 , IC card 1 and the reader writer 2 perform mutual recognition with the authentication key specified by the reader writer 2 corresponding to the service ID of the service identified by processing of step S1 of drawing 15 , and step S2.

[0114] For example, it makes to perform high-speed processing by authentication processing based on a common key into a default, and when the version of a common key is old, based on a public key, it may be made to carry out authentication processing, when two kinds of authentication keys, a common key and a public key, are prepared to a certain service.

[0115] Next, with reference to the flow chart of drawing 22 , authentication key discernment processing of the reader writer 2 in case two kinds of authentication keys, a common key and a public key, are prepared is explained to the service corresponding to the service ID of the service identified by processing of step S1 of drawing 15 and step S2 which are performed in step S3 of drawing 15 .

[0116] The control section 101 of the reader writer 2 transmits the common key version information-requirements command of the authentication key corresponding to the service ID of the service identified by processing of step S1 of drawing 15 , and step S2 to IC card 1 through the communications department 91, and receives the common key version information which IC card 1 transmitted through the communications department 91 in step S92 of drawing 23 mentioned later in step S82 in step S81.

[0117] In step S83, a control section 101 judges whether a common key version is effective based on the common key version information received in step S82. In step S83, when it is judged that a common key version is effective, after a control section 101 transmits a mutual recognition initiation command with a common key to IC card 1, controlling the common key processing section 112 of the cipher-processing section 102, starting mutual recognition with a common key, sharing IC card 1 and the session key Kses and completing mutual recognition, processing is ended in step S84.

[0118] In step S83, when it is judged that a common key version is not effective, after a control section 101 transmits the mutual recognition initiation command by the public key to IC card 1, controlling the public key processing section 111 of the cipher-processing section 102, starting the mutual recognition by the public key, sharing IC card 1 and the session key Kses and completing mutual recognition, processing is ended in step S85.

[0119] Next, with reference to the flow chart of drawing 23 , the authentication key discernment processing of IC card 1 performed in parallel to authentication key discernment processing of the reader writer 2 explained using drawing 22 is explained in step S4 of drawing 15 . In addition, although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4 , same processing is performed fundamentally.

[0120] In step S91, in step S81 of drawing 22 , the control section 31 of IC card 1 receives the common key version information-requirements command which the reader writer 2 transmitted, and transmits common key version information to the reader writer 2 through the communications department 21 in step S92.

[0121] A control section 31 judges whether the mutual recognition initiation command which received the mutual recognition initiation command which the reader writer 2 transmitted, and was received in step S93 in step S94 is a mutual

recognition initiation command with a common key in step S84 or step S85 of drawing 22 in step S93.

[0122] In step S94, when it is judged that it is a mutual recognition initiation command with a common key, after a control section 31 controls the common key processing section 42 of the cipher-processing section 33, starting mutual recognition with a common key, sharing the reader writer 2 and the session key Kses and completing mutual recognition, processing is ended in step S95.

[0123] In step S94, when it is judged that it is not a mutual recognition initiation command with a common key (that is, it is a mutual recognition initiation command by the public key), after a control section 31 controls the public key processing section 41 of the cipher-processing section 33, starting the mutual recognition by the public key, sharing the reader writer 2 and the session key Kses and completing mutual recognition, processing is ended in step S96.

[0124] By processing explained using drawing 22 and drawing 23, IC card 1 and the reader writer 2 perform mutual recognition using a public key, when it is going to perform mutual recognition with a common key with a quick authentication rate first and mutual recognition with a common key cannot be performed (for example, when the version of a corresponding common key is old etc.).

[0125] Mutual recognition by the public key is performed in processing of step

S85 of drawing 22 , and step S96 of drawing 23 . The certificate of the reader writer 2 shown in drawing 24 (A) is memorized by SRA46 of the memory 103 of the reader writer 2. Moreover, the certificate of IC card 1 shown in drawing 24 (B) is memorized by SRA46 of the memory 32 of IC card 1.

[0126] As shown in drawing 24 (A) and drawing 24 (B), in each certificate The version number of a certificate, the serial number of the certificate which a certificate authority assigns, the algorithm and parameter that were used for the signature, The identifier of a certificate authority, the expiration date of a certificate, the reader writer 2, or the identifier of IC card 1 (ID), By making an irreversible Hash Function (data compression function) which used and explained drawing 5 to the public key Kpsp of the reader writer 2 or the public key Kpu of IC card 1, and the whole message act It consists of digital signatures which created the message digest and were created by enciphering a message digest with the private key Ksca of a certificate authority.

[0127] Next, signature generation processing is explained with reference to the flow chart of drawing 25 . Here, the case where a digital signature is generated is explained using an elliptic curve cryptosystem method (ellipse DSA signature). Here, also in the reader writer 2, although the control section 31 of IC card 1 explains the processing performed by controlling DSA signature generation / verification section 72 of the public key processing section 41, since same

processing is performed, the explanation about processing of the reader writer 2 is omitted.

[0128] In step S101, a control section 31 recognizes a parameter required for signature generation processing. namely, p -- the characteristic, and a and b -- the multiplier of an elliptic curve, and an elliptic curve -- let a message and K_s as a private key and let $[y^2=x^3+ax+b$ and G / the base point on an elliptic curve, and $r]$ G and K_sG be public keys for the order of G , and M .

[0129] In step S102, DSA signature generation / verification section 72 of the public key processing section 41 is the random-number generation section which is not illustrated, it generates u used as $0 < u < r$, u Doubles a public key G using the random number u generated in step S102 in step S103, and computes V used as $V=uG= (X_v, Y_v)$.

[0130] In step S104, DSA signature generation / verification section 72 computes $c=X_v \bmod r$, and judges whether it is $c=0$ in step S105 based on the count result of S104. In step S105, when it is judged that it is $c=0$, as for processing, return and processing after it are repeated by step S102.

[0131] It computes $[f=SHA^{-1}(M)$ which is / in / when it is judged in step S105 that it is not $c=0$ / step S106 / the hash value of Message M , (SHA-1 being used as a Hash Function here), and $]$, it sets to step S107, and DSA signature generation / verification section 72 is $d= [(f+cK_s) / u]. \bmod r$ is calculated.

[0132] In step S108, DSA signature generation / verification section 72 judges whether it is $d=0$ based on the count result of step S107. In step S108, when it is judged that it is $d=0$, as for processing, return and processing after it are repeated by step S102. In step S108, when it is judged that it is not $d=0$, in step S109, DSA signature generation / verification section 72 sets signature data to (c, d), and processing is ended.

[0133] Thus, the reader writer 2 which received the digital signature generated in IC card 1 carries out processing which verifies the digital signature which received. Signature verification processing is explained with reference to the flow chart of drawing 26. Here, also in IC card 1, although the control section 101 of the reader writer 2 explains the processing performed by controlling DSA signature generation / verification section 72 of the public key processing section 41, since same processing is performed, the explanation about processing of IC card 1 is omitted.

[0134] In step S111, a control section 101 recognizes a parameter required for signature generation processing. namely, p -- the characteristic, and a and b -- the multiplier of an elliptic curve, and an elliptic curve -- let a message and K_s as a private key and let $[y^2=x^3+ax+b$ and G / the base point on an elliptic curve, and $r]$ G and K_sG be public keys for the order of G , and M .

[0135] DSA signature generation / verification section 72 of the public key

processing section 41 judges whether they are $0 < c < r$ and $0 < d < r$ in step S112 based on the value of c and d of the received signature data.

[0136] In step S112, when it is judged that they are not $0 < c < r$ and $0 < d < r$, processing progresses to step S120. In step S112, when it is judged that they are $0 < c < r$ and $0 < d < r$, in step S113, DSA signature generation / verification section 72 computes $f = \text{SHA-1}(M)$ which is the hash value of Message M , and calculates $h = 1/d \bmod r$ in step S114.

[0137] Using the value of h computed in step S114, in step S115, DSA signature generation / verification section 72 computes $h_1 = fh$ and $h_2 = ch \bmod r$, and computes $P = (X_p, Y_p) = h_1 G + h_2 K_s G$ in step S116.

[0138] In step S117, DSA signature generation / verification section 72 judges whether the value of P is an infinite point from the calculation result of step S116. Here, when the value of P is an infinite point, it is possible to judge whether the value of P is an infinite point in step S116 based on the ability not to acquire the solution of $h_1 G + h_2 K_s G$. In step S117, when it is judged that P is an infinite point, processing progresses to step S120.

[0139] In step S117, when the value of P is judged not to be an infinite point, in step S118, DSA signature generation / verification section 72 judges whether $c = X_p \bmod r$ is realized. In step S118, when it is judged that $c = X_p \bmod r$ is not realized, processing progresses to step S120.

[0140] In step S118, when it is judged that $c = Xp \bmod r$ is realized, in step S119, DSA signature generation / verification section 72 judges the received signature to be the right, and processing is ended.

[0141] When it is judged that p is an infinite point in step S117 when it is judged in step S112 that they are not $0 < c < r$ and $0 < d < r$, or when it is judged in step S118 that $c = Xp \bmod r$ is not realized, in step S120, it judges that DSA signature generation / verification section 72 of the received signature is not right, and processing is ended.

[0142] Moreover, authentication key discernment is performed using the key information for authentication that it explained using drawing 7 (B). When two or more authentication keys by which the level division was carried out to a certain service are stored, authentication processing is preferentially started from the key of a low, and the version of the key is judged, and when the version of the key is old, it may be made to perform authentication processing using the authentication key of higher level.

[0143] Next, authentication key discernment processing of the reader writer 2 in case two or more authentication keys which are performed in step S3 of drawing 15 and by which the level division was carried out to a certain service are stored with reference to the flow chart of drawing 27 is explained.

[0144] In step S131, through the communications department 91, the control

section 101 of the reader writer 2 transmits a key level negotiation command to IC card 1, and receives key version information V in level N which IC card 1 transmits through the communications department 91 in step S143 of drawing 28 mentioned later in step S132.

[0145] In step S133, a control section 101 judges whether the level N of key version information V which received in step S132 is $N > 0$. In step S133, when it is judged that it is not $N > 0$, processing progresses to step S137.

[0146] In step S133, when it is judged that it is $N > 0$, in step S134, a control section 101 judges whether the key version information in level N is effective based on key version information V which received in step S132.

[0147] In step S134, when it is judged that the key version in level N is not effective, in step S135, a control section 101 transmits a NACK signal to IC card 1 through the communications department 91, and, as for processing, return and processing after it are repeated by step S132 (namely, when it is judged that the version of a key is old).

[0148] In step S134, when it is judged that the key version in level N is effective, in step S136, a control section 101 transmits an ACK signal to IC card 1 through the communications department 91, and processing is ended.

[0149] In step S133, when it is judged that it is not $N > 0$, in step S137, the same processing as step S16 of drawing 16 is made, and processing is ended.

[0150] Next, with reference to the flow chart of drawing 28 , the authentication key discernment processing of IC card 1 performed in parallel to authentication key discernment processing of the reader writer 2 explained using drawing 27 is explained. In addition, although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4 , same processing is performed fundamentally.

[0151] In step S141, in step S131 of drawing 27 , the control section 31 of IC card 1 receives the key level negotiation command which the reader writer 2 transmitted, and sets the present key level N to $N = 1$ in step S142.

[0152] In step S143, a control section 31 transmits key version information V in the present key level N and its level to the reader writer 2 through the communications department 21, and receives the data which the reader writer 2 transmitted in step S135 or step S136 of drawing 27 in step S144.

[0153] In step S145, a control section 31 judges whether the signal received from the reader writer 2 is an ACK signal in step S144. In step S145, when it is judged that the signal received from the reader writer 2 is not an ACK signal, in step S146, a control section 31 considers as $N = N + 1$, and judges whether the value of N is over the predetermined maximum level in step S147.

[0154] In step S147, when it is judged that N is not over the maximum level, as

for processing, return and processing after it are repeated by step S143. In step S147, when it is judged that N is over the maximum level, in step S148, a control section 31 sets current level to $N = 0$ ($N = 0$ shall show an exception condition), and, as for processing, return and processing after it are repeated by step S143.

[0155] In step S145, when it is judged that the signal received from the reader writer 2 is an ACK signal, processing is ended.

[0156] Although the processing about IC card 1, service discernment of the reader writer 2, and authentication key discernment was explained using drawing 15 thru/or drawing 28 For example, when equipping with IC card 1 and performing registration of new service, and when deletion of service was performed to the reader writer 2-11 for service registration explained using drawing 2 , as it explained to it using drawing 10 In order to perform authentication processing using the authentication key Kreg for service registration memorized by the memory 103 of the reader writer 2-11 for service registration, it is not necessary to use mutual recognition processing which was explained using drawing 15 thru/or drawing 28 .

[0157] Next, with reference to the flow chart of drawing 29 , service registration processing of the reader writer 2-11 for service registration is explained.

[0158] In step S151, through the communications department 91, the control section 101 of the reader writer 2-11 for service registration transmits a service

registration command to IC card 1, performs IC card 1 and mutual recognition with the key Kreg for service registration in step S152, and shares the session key Kses.

[0159] In step S153, a control section 101 transmits a free-area check command to IC card 1 through the communications department 91, and receives the data transmitted from IC card 1 in step S175 or step S176 of drawing 30 mentioned later in step S154.

[0160] In step S155, a control section 101 judges whether the signal received from IC card 1 is an ACK signal in step S154. When the signal received from IC card 1 is judged to be an ACK signal, in step S155, in step S156, a control section 101 controls the common key processing section 112 of the cipher-processing section 102, makes the registration data newly registered into the memory 32 of IC card 1 encipher with the session key Kses, and transmits encryption data to IC card 1 through the communications department 91 in step S157.

[0161] The notice of the completion of data registration to which IC card 1 transmitted the control section 101 in step S180 of drawing 30 later mentioned in step S158 is received through the communications department 91, the service deletion authorization flag by service authentication is transmitted in step S159, and processing is ended.

[0162] In step S155, when the signal received from IC card 1 is judged not to be an ACK signal, in step S160, the same processing as step S16 of drawing 16 is made, and processing is ended.

[0163] Next, with reference to the flow chart of drawing 30 , the service registration processing of IC card 1 performed in parallel to service registration processing of the reader writer 2-11 for service registration in which it explained using drawing 29 is explained. In addition, although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4 , same processing is performed fundamentally.

[0164] In step S171, the control section 31 of IC card 1 receives the service registration command which the reader writer 2-11 for service registration transmitted in step S151 of drawing 29 through the communications department 21.

[0165] A control section 31 performs mutual recognition with the key Kreg for service registration, shares the session key Kses with IC card 1, and receives the free-area check command which the reader writer 2-11 for service registration transmitted in step S153 of drawing 29 through the communications department 21 in step S173 in step S172.

[0166] In step S174, a control section 31 judges whether the free area for

registration data is in SRA46 of memory 32. In step S174, when it is judged that there is no free area, in step S175, a control section 31 transmits a NACK signal through the communications department 21 at the reader writer 2-11 for service registration, and processing is ended.

[0167] In step S174, when it is judged that there is a free area, in step S176, a control section 31 transmits an ACK signal to the reader writer 2-11 for service registration through the communications department 21.

[0168] A control section 31 receives the encryption data which the reader writer 2-11 for service registration transmitted through the communications department 21, controls the common key processing section 42 of the cipher-processing section 33 in step S178, and makes the encryption data received in step S177 decode in step S157 of drawing 29 in step S177 using the session key Kses.

[0169] A control section 31 supplies the data decoded with the session key Kses to memory 32, and makes them register into the Service Individual Info field and SRT45 of SRA46 in step S178 in step S179.

[0170] In step S180, through the communications department 21, a control section 31 notifies the completion of registration of data to the reader writer 2-11 for service registration, and sets it to step S181. In step S159 of drawing 29, the reader writer 2-11 for service registration transmitted. The service deletion authorization flag by service authentication is received, a service deletion

authorization flag is set as the Service Individual Info field of SRA46 of memory 32, and processing is ended.

[0171] Next, with reference to the flow chart of drawing 31 , the service deletion of the reader writer 2-11 for service registration is explained.

[0172] In step S191, the control section 101 of the reader writer 2-11 for service registration receives the input of the service ID corresponding to the service to delete which the user inputted using the input section 106 (here, the service whose corresponding service ID is ID_S shall be deleted).

[0173] In step S192, the same processing as step S152 of drawing 29 is made. A control section 101 judges whether the error message which transmitted ID_S region Delete command to IC card 1, and IC card 1 transmitted to it in step S205 of drawing 32 mentioned later in step S194 was received through the communications department 91 in step S193.

[0174] In step S194, when it is judged that the error message was received, in step S195, the same processing as step S16 of drawing 16 is made, and processing is ended. In step S194, when it is judged that an error message was not received, processing is ended.

[0175] Next, with reference to the flow chart of drawing 32 , the service deletion of IC card 1 performed in parallel to the service deletion of the reader writer 2-11 for service registration explained using drawing 31 is explained. In addition,

although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4 , same processing is performed fundamentally.

[0176] In step S201, the same processing as step S172 of drawing 30 is performed. The control section 31 of IC card 1 judges whether the justification of ID_S region Delete command which received in step S202 was verified in step S193 of drawing 31 in step S202 by receiving ID_S region Delete command which the reader writer 2-11 for service registration transmitted, and checking whether there are any data corresponding to ID_S region in step S203 etc.

[0177] In step S203, when it is judged that the justification of ID_S region Delete command was verified, in step S204, a control section 31 deletes the field corresponding to ID_S of memory 32 from SRT45 and SRA46, and processing is ended.

[0178] In step S203, when it is judged that the justification of ID_S region Delete command was not verified, in step S205, a control section 31 transmits an error message to the reader writer 2-11 for service registration through the communications department 21, and processing is ended.

[0179] Service deletion explained using drawing 31 and drawing 32 can also be performed with the general reader writer 2-12 and IC card 1. With reference to the flow chart of drawing 33 , the service deletion of the general reader writer

2-12 is explained.

[0180] In step S211, service discernment processing of the reader writer 2 explained using drawing 16 or drawing 18 is performed, in step S212, authentication key discernment processing of the reader writer 2 explained using drawing 20 , drawing 22 , or drawing 27 is performed, and the same processing as step S193 of drawing 31 is performed in step S213.

[0181] In step S214, the control section 101 of the general reader writer 2-12 receives the signal which IC card 1 transmits in step S227 or step S228 of drawing 34 mentioned later. And in step S215 and step S216, the same processing as step S15 of drawing 16 and step S16 is performed, and processing is ended.

[0182] Next, with reference to the flow chart of drawing 34 , the service deletion of IC card 1 performed in parallel to the service deletion of the general reader writer 2-12 explained using drawing 33 is explained. In addition, although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4 , same processing is performed fundamentally.

[0183] In step S221, service discernment processing of IC card 1 in which it explained using drawing 17 or drawing 19 is performed, and authentication key discernment processing of IC card 1 explained using drawing 21 , drawing 23 ,

or drawing 28 is performed in step S232.

[0184] In step S223, a control section 31 receives ID_S region Delete command which the general reader writer 2-12 transmitted through the communications department 21 in step S213 of drawing 33 . In step S224, the same processing as step S203 of drawing 32 is performed.

[0185] In step S224, when it is judged that the justification of a command was not verified, processing progresses to step S228. In step S224, when it is judged that the justification of a command was verified, in step S225, a control section 31 judges whether the service deletion authorization flag is set as the Service Individual Info field of SRA46 of memory 32.

[0186] In step S225, when it is judged that the service deletion authorization flag is not set up, processing progresses to step S228. In step S225, when it is judged that the service deletion authorization flag is set up, in step S226, the same processing as step S204 of drawing 32 is made, in step S227, a control section 31 transmits an ACK signal to the general reader writer 2-12 through the communications department 21, and processing is ended.

[0187] In step S224, when it is judged that the justification of a command was not verified, or when it is judged in step S225 that the service deletion authorization flag is not set up, in step S228, a control section 31 transmits a NACK signal to the general reader writer 2-12 through the communications

department 21, and processing is ended.

[0188] Next, service acquisition processing of the general reader writer 2-12 performed when a user receives the service registered into IC card 1 by the general reader writer 2-12 with reference to the flow chart of drawing 35 is explained.

[0189] In step S231, service discernment processing of the reader writer 2 explained using drawing 16 or drawing 18 is performed, and authentication key discernment processing of the reader writer 2 explained using drawing 20 , drawing 22 , or drawing 27 is performed in step S232.

[0190] In step S233, the control section 101 of the general reader writer 2-12 transmits the data demand command of ID_S region to IC card 1 through the communications department 91.

[0191] A control section 101 receives the data transmitted from IC card 1, controls the common key processing section 112 of the cipher-processing section 102 in step S235, and makes the encryption data received in step S234 decode in step S245 of drawing 36 mentioned later in step S234 using the session key Kses. A control section 101 performs predetermined data processing, such as subtraction of cybermoney, and addition, using the decoded data, and processing is ended.

[0192] Next, with reference to the flow chart of drawing 36 , the service data

acquisition processing of IC card 1 performed in parallel to service data acquisition processing of the general reader writer 2-12 in which it explained using drawing 35 is explained. In addition, although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4 , same processing is performed fundamentally.

[0193] In step S241, service discernment processing of IC card 1 in which it explained using drawing 17 or drawing 19 is performed, and authentication key discernment processing of IC card 1 explained using drawing 21 , drawing 23 , or drawing 28 is performed in step S232.

[0194] In step S243, the control section 31 of IC card 1 receives the data demand command of ID_S region which the general reader writer 2-12 transmitted in step S233 of drawing 35 through the communications department 21. In step S244, a control section 31 controls the common key processing section 42 of the cipher-processing section 33, makes the data registered into the field corresponding to ID_S of memory 32 encipher using the session key Kses, and transmits the data enciphered through the communications department 21 to the general reader writer 2-12 in step S245, and processing is ended.

[0195] Moreover, in IC card 1 and the general reader writer 2-12, when the

permission information corresponding to SRT45 explained using drawing 8 when transfer of the information about a certain service was made is recorded, it is possible to deliver and receive information about the service except transfer of the present information being made. With reference to the flow chart of drawing 37, the service data acquisition processing of the general reader writer 2-12 performed during activation of the service corresponding to the service ID of those other than ID_S is explained.

[0196] In step S251 thru/or step S254, the same processing as step S231 of drawing 35 thru/or step S234 is performed. In step S255, the data which the control section 101 of the general reader writer 2-12 received from IC card 1 in step S254 judge whether it is a NACK signal.

[0197] In step S255, when the received data are judged not to be a NACK signal, in step S256, the same processing as step S235 of drawing 35 is performed, and processing is ended. In step S255, when the received data are judged to be a NACK signal, the same processing as step S16 of drawing 16 is made, and processing is ended.

[0198] Next, with reference to the flow chart of drawing 38, the service data acquisition processing of IC card 1 performed in parallel to service data acquisition processing of the general reader writer 2-12 in which it explained using drawing 37 is explained. In addition, although IC card 1 explained also

here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4 , same processing is performed fundamentally.

[0199] In step S261 thru/or step S263, the same processing as step S241 of drawing 34 thru/or step S243 is performed. In addition, at step S261, authentication of different service ID_T from service ID_S shall be performed. In step S264, the control section 31 of IC card 1 judges whether ID_S region corresponding to the data demand command received to SRT45 and SRA46 of memory 32 in step S263 is registered. In step S264, when it is judged that ID_S region is not registered, processing progresses to step S269.

[0200] When it is judged in step S264 that ID_S region is registered, a control section 31 In step S265, from the permission information field corresponding to ID_S of SRT45 of memory 32, acquire the permission information on ID_S and it sets to step S266. It judges whether reading of the data of ID_S is permitted at the time of ID_T authentication (). That is, it judges whether read-out authorization of data, i.e., ro, and rw are indicated in the permission information field corresponding to ID_S of SRT45 at the time of authentication by ID_T. In step S266, when it is judged that reading of data is not permitted, processing progresses to step S269.

[0201] In step S266, when it is judged that reading of data is permitted, in step

S267 and step S268, the same processing as step S244 of drawing 36 and step S245 is performed, and processing is ended.

[0202] In step S264, when it is judged that ID_S region is not registered, or when it is judged in step S266 that reading of data is not permitted, in step S269, a control section 31 transmits a NACK signal to the general reader writer 2-12 through the communications department 21, and processing is ended.

[0203] After data are acquired from IC card 1 by the general reader writer 2-12 and predetermined processing is made by service data acquisition processing in which it explained using drawing 35 thru/or drawing 48 , the general reader writer 2-12 performs processing which writes in data to the predetermined field of SRT45 of the memory 32 of IC card 1, or SRA46 if needed.

[0204] Next, with reference to the flow chart of drawing 39 , service data write-in processing of the general reader writer 2-12 is explained.

[0205] In step S281, service discernment processing of the reader writer 2 explained using drawing 16 or drawing 18 is performed, and authentication key discernment processing of the reader writer 2 explained using drawing 20 , drawing 22 , or drawing 27 is performed in step S282.

[0206] The control section 101 of the general reader writer 2-12 In step S283, in order to write in the memory 32 of IC card 1 Control the common key processing section 112 of the cipher-processing section 102, make it encipher using the

session key Kses, and the data transmitted to IC card 1 are set to step S284.

The data enciphered as the data write command in step S284 are transmitted to IC card 1 through the communications department 91, and processing is ended.

[0207] Next, with reference to the flow chart of drawing 40 , the service data write-in processing of IC card 1 performed in parallel to service data write-in processing of the general reader writer 2-12 in which it explained using drawing 39 is explained. In addition, although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4, same processing is performed fundamentally.

[0208] In step S291, service discernment processing of IC card 1 in which it explained using drawing 17 or drawing 19 is performed, and authentication key discernment processing of IC card 1 explained using drawing 21, drawing 23, or drawing 28 is performed in step S232.

[0209] In step S293, a control section 31 receives the data write command and encryption data which the general reader writer 2-12 transmitted in step S284 of drawing 39 through the communications department 21. A control section 31 writes the data which were made to decode the data which controlled the common key processing section 42 of the cipher-processing section 33, and were received using the session key Kses, and decoded them in step S295 in

step S294 in the service storing field corresponding to ID_S of SRT45 and SRA46 of memory 32, and processing is ended.

[0210] Moreover, in IC card 1 and the general reader writer 2-12, when the permission information corresponding to SRT45 explained using drawing 8 when transfer of the information about a certain service was made is recorded, it is possible to perform service data write-in processing about the service except transfer of the present information being made as well as service data acquisition processing in which it explained using drawing 37 and drawing 38. With reference to the flow chart of drawing 41, the service data write-in processing of the general reader writer 2-12 performed during activation of the service corresponding to the service ID of those other than ID_S is explained.

[0211] In step S301 thru/or step S304, the same processing as step S281 of drawing 39 thru/or step S284 is performed. And in step S305 and step S306, the same processing as step S15 of drawing 16 and step S16 is made, and processing is ended.

[0212] Next, with reference to the flow chart of drawing 42, the service data write-in processing of IC card 1 performed in parallel to service data write-in processing of the general reader writer 2-12 in which it explained using drawing 41 is explained. In addition, although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is

performed with IC card 1 explained using drawing 4, same processing is performed fundamentally.

[0213] In step S311 thru/or step S313, the same processing as step S291 of drawing 40 thru/or step S293 is performed. In addition, at step S311, authentication of different service ID_T from service ID_S shall be performed. In step S314 and step S315, the same processing as step S264 of drawing 38 and step S265 is made, and in step S314, when it is judged that ID_S region is not registered, processing progresses to step S320.

[0214] In step S316, a control section 31 judges whether the writing of data is permitted to service of ID_S at the time of ID_T authentication (that is, it judges whether write-in authorization of the data at the time of ID_T authentication, i.e., rw, is indicated in the permission information field corresponding to ID_S of SRT45). In step S316, when it is judged that the writing of data is not permitted, processing progresses to step S320.

[0215] In step S316, when it is judged that the writing of data is permitted, in step S317 and step S318, the same processing as step S294 of drawing 40 and step S295 is performed. In step S319, a control section 31 transmits an ACK signal to the general reader writer 2-12 through the communications department 21, and processing is ended.

[0216] In step S314, when it is judged that ID_S region is not registered, or when

it is judged in step S316 that the writing of data is not permitted, in step S320, a control section 31 transmits a NACK signal to the general reader writer 2-12 through the communications department 21, and processing is ended.

[0217] As explained above, in order to equip the general reader writer 2-12 with IC card 1 and to receive various services in it, authentication processing must be performed using the common key defined for every service, or a public key. These authentication keys are often upgraded for maintenance of security (that is, a key is changed). A user must be made to have to upgrade the authentication key registered into IC card 1 which he has managed to the authentication key of the version near the newest as much as possible by equipping with IC card 1 the reader writer 2-14 for version up explained using drawing 2, or the general reader writer 2-12, and performing key version up processing later mentioned using drawing 43 thru/or drawing 47.

[0218] Next, with reference to drawing 43, key version up processing of the reader writer 2-14 for version up performed using the key for version up (key Kake_vup for version up explained using drawing 6 and drawing 14) defined for every service is explained.

[0219] In step S331, service discernment processing of the reader writer 2 explained using drawing 16 or drawing 18 is performed, and authentication key discernment processing of the reader writer 2 explained using drawing 20,

drawing 22, or drawing 27 is performed in step S332.

[0220] In step S333, the control section 101 of the reader writer 2-14 for version up controls the common key processing section 112 of the cipher-processing section 102, makes the authentication key ID corresponding to the authentication key which upgrades encipher using the session key Kses, and transmits to IC card 1. In step S334, a control section 101 receives the signal which IC card 1 transmits in step S355 or step S360 of drawing 44 mentioned later.

[0221] In step S335, a control section 101 judges whether the signal received from IC card 1 in step S334 is an ACK signal. In step S335, when the received signal is judged not to be an ACK signal, processing progresses to step S339. In step S335, when the received signal is judged to be an ACK signal, in step S336, read the authentication key Kake from memory 103, control the common key processing section 112 of the cipher-processing section 102, it is made to encipher it as the latest version information corresponding to the authentication key which upgrades using the session key Kses, and a control section 101 transmits to IC card 1 through the communications department 91.

[0222] And in step S337, the signal transmitted in step S359 or step S360 of 44 which IC card 1 mentions later is received. In step S338, the same processing as step S335 is made, and in step S338, when the received signal is judged to be

an ACK signal, processing is ended. In step S335 and step S338, when the received signal is judged not to be an ACK signal, in step S339, the same processing as step S16 of drawing 16 is made, and processing is ended.

[0223] Next, with reference to the flow chart of drawing 44, the key version up processing of IC card 1 performed in parallel to key version up processing of the reader writer 2-14 for version up in which it explained using drawing 43 is explained. In addition, although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4, same processing is performed fundamentally.

[0224] In step S351, service discernment processing of IC card 1 in which it explained using drawing 17 or drawing 19 is performed, and authentication key discernment processing of IC card 1 explained using drawing 21, drawing 23, or drawing 28 is performed in step S352.

[0225] A control section 31 receives the enciphered authentication key ID which the reader writer 2-14 for version up transmitted in step S333 of drawing 43 through the communications department 21, controls the common key processing section 42 of the cipher-processing section 33, and makes the received data decode in step S353 using the session key Kses. In step S354, a control section 31 judges whether the authentication key ID corresponding to

ID_S of SRT45 and SRA46 of memory 32 exists based on the decoded data. In step S354, when it is judged that the authentication key ID does not exist, processing progresses to step S360.

[0226] When it is judged in step S354 that the authentication key ID exists, a control section 31 In step S355, through the communications department 21, transmit an ACK signal to the reader writer 2-14 for version up, and it sets to step S356. In step S336 of drawing 43, the reader writer 2-14 for version up transmitted. The latest version information and the authentication key Kake which were enciphered are received through the communications department 21, the common key processing section 42 of the cipher-processing section 33 is controlled, and the received version information is made to decode using the session key Kses.

[0227] In step S357, the version information received based on the data which the control section 31 decoded judges whether it is the right (that is, is he a version higher than the version information of the already held authentication key or not?). In step S357, when version information is judged not to be right, processing progresses to step S360.

[0228] When judged as the right, in step S357, version information a control section 31 Control the common key processing section 42 of the cipher-processing section 33, make the authentication key Kake decode using

the session key Kses, write in the field to which the authentication key Kake in SRA46 of memory 32 is indicated, and it sets to step S359. An ACK signal is transmitted to the reader writer 2-14 for version up through the communications department 21, and processing is ended.

[0229] In step S354, when it is judged that the authentication key ID does not exist, and when version information is judged not to be right in step S357, in step S360, a control section 31 transmits a NACK signal to the reader writer 2-14 for version up through the communications department 21, and processing is ended.

[0230] Moreover, in IC card 1 and the general reader writer 2-12, when transfer of the information about a certain service is made, it sets. When the permission information corresponding to SRT45 explained using drawing 8 is recorded, It is possible to perform key version up processing about the service except transfer of the present information being made as well as service data acquisition processing in which it explained using drawing 37 and drawing 38, and service data write-in processing in which it explained using drawing 41 and drawing 42. With reference to the flow chart of drawing 45, the key version up processing of the general reader writer 2-12 performed during activation of the service corresponding to the service ID of those other than ID_S is explained.

[0231] In step S371 and step S372, the same processing as step S331 of drawing 44 and step S332 is performed. And the control section 101 of the

general reader writer 2-12 In step S373, transmit to IC card 1 through the communications department 91, and the version up command of the authentication key of the service corresponding to ID_S is set to step S374. In step S397 of drawing 46 mentioned later, or step S405 of drawing 47, the signal which received the data which IC card 1 transmits and was received from IC card 1 in step S375 judges whether it is an ACK signal.

[0232] In step S375, when the received signal is judged not to be an ACK signal, processing progresses to step S382. In step S375, when the received signal is judged to be an ACK signal, in step S376 thru/or step S382, the same processing as step S333 of drawing 43 thru/or step S339 is made, and processing is ended.

[0233] Next, with reference to the flow chart of drawing 46 and drawing 47, the key version up processing of IC card 1 performed in parallel to key version up processing of the reader writer 2-14 for version up in which it explained using drawing 45 is explained. In addition, although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4, same processing is performed fundamentally.

[0234] In step S391 and step S392, the same processing as step S351 of drawing 44 and step S352 is performed. In addition, at step S391, authentication

of different service ID_T from service ID_S shall be performed. In step S393, a control section 31 receives the version up command of the authentication key of ID_S which the reader writer 2-14 for version up transmitted in step S373 of drawing 45.

[0235] In step S394 and step S395, the same processing as step S264 of drawing 38 and step S265 is made, and in step S394, when it is judged that ID_S region is not registered, processing progresses to step S405.

[0236] In step S396, a control section 31 judges whether version up of the authentication key of ID_S is permitted at the time of ID_T authentication (that is, it judges whether authorization of vup at the time of ID_T authentication is indicated in the permission information field corresponding to ID_S of SRT45). In step S396, when it is judged that version up of an authentication key is not permitted, processing progresses to step S405.

[0237] In step S396, when it is judged that version up of an authentication key is permitted, in step S397, a control section 31 transmits an ACK signal to the reader writer 2-14 for version up through the communications department 21.

[0238] And in step S398 thru/or step S405, the same processing as step S353 of drawing 44 thru/or step S360 is performed, and processing is ended.

[0239] Next, with reference to the flow chart of drawing 48 thru/or drawing 51, the intermodule communication explained using drawing 13 is explained.

Intermodule communication is performed by IC card 1 explained using drawing 4, and the reader writer 2-13 for intermodule communications. Here, it considers as the common key module 122 which explained the communications department 51 of IC card 1 explained using drawing 4, and the common key service processing section 52 using drawing 13, and explains as a public key module 121 which explained the communications department 53 which explained using drawing 4, and the public key service processing section 54 using drawing 13.

[0240] First, the intermodule communication in the case of differing the session key which the common key module 122 shares with the reader writer 2-13 for intermodule communications, and the session key which the public key module 121 shares with the reader writer 2-13 for intermodule communications with reference to the flow chart of drawing 48 is explained.

[0241] In step S411, the reader writer 2-13 for intermodule communications performs service discernment processing of the reader writer 2 explained using drawing 16 or drawing 18, and in step S412, the public key module 121 of IC card 1 performs service discernment processing of IC card 1 in which it explained using drawing 17 or drawing 19, and it shares the session key K_{ses1} with the inter module reader writer 2-13 between the public key modules 121.

[0242] In step S413 the reader writer 2-13 for intermodule communications Service discernment processing of the reader writer 2 explained using drawing

16 or drawing 18 is performed, and it sets to step S414. The common key module 122 of IC card 1 Service discernment processing of IC card 1 in which it explained using drawing 17 or drawing 19 is performed, and the session key Kses2 is shared with the inter module reader writer 2-13 between the common key modules 122.

[0243] In step S415, the control section 101 of the reader writer 2-13 for intermodule communications judges whether two cards, the public key module 121 and the common key module 122, ID were in agreement based on the card ID of IC card 1 obtained in service discernment processing of the reader writer 2 performed in step S411 and step S413. In step S415, when it is judged that Card ID is not in agreement, in step S416, the same processing as step S16 of drawing 16 is performed.

[0244] In step S415, when it is judged that two cards ID are in agreement, in step S417, the control section 101 of the reader writer 2-13 for intermodule communications transmits a module data migration command to the public key module 121.

[0245] In step S418, the control section 61 of the public key module 121 receives a module data migration initiation command from the reader writer 2-13 for intermodule communications, controls the common key processing section 42 of the cipher-processing section 33, makes the data which move encipher with the

session key Kses1, is step S419 and transmits encryption data to the reader writer 2-13 for intermodule communications.

[0246] In step S420, the control section 101 of the reader writer 2-13 for intermodule communications decodes the data which controlled the common key processing section 112 of the cipher-processing section 102, and were received with the session key Kses1, makes data encipher with the session key Kses2 in step S421, and transmits to the common key module 122. In step S422, the control section 61 of the common key module 122 makes the data which controlled the common key processing section 42 of the cipher-processing section 63, and were received decode with the session key Kses2, and the data decoded in step S423 are saved to the field to which memory 62 corresponds, and it uses them.

[0247] Next, with reference to the flow chart of drawing 49, intermodule communication when the session key which the common key module 122 shares with the reader writer 2-13 for intermodule communications, and the session key which the public key module 121 shares with the reader writer 2-13 for intermodule communications are the same is explained.

[0248] In step S431, the reader writer 2-13 for intermodule communications performs service discernment processing of the reader writer 2 explained using drawing 16 or drawing 18, and in step S432, the public key module 121 of IC

card 1 performs service discernment processing of IC card 1 in which it explained using drawing 17 or drawing 19, and it shares the session key Kses1 with the inter module reader writer 2-13 between the public key modules 121.

[0249] In step S433 the reader writer 2-13 for intermodule communications Service discernment processing of the reader writer 2 explained using drawing 16 or drawing 18 is performed, and it sets to step S434. The common key module 122 of IC card 1 Service discernment processing of IC card 1 in which it explained using drawing 17 or drawing 19 is performed, and the session key Kses1 is shared with the inter module reader writer 2-13 between the common key modules 122.

[0250] In step S435 thru/or step S439, the same processing as step S415 of drawing 48 thru/or step S419 is performed. And in step S440, the control section 101 of the reader writer 2-13 for intermodule communications transmits the received data to the common key module 122. After enciphering the decoded data with the session key Kses2, it transmitted to the common key module 122, but since the common key module 122 also has the session key Kses1, these processings become unnecessary [decode the received data with the session key Kses1, and / the module] in step S420 and step S421 of drawing 48, here.

[0251] In step S411, the control section 61 of the common key module 122 decodes the data which controlled the cipher-processing section 63 and were

received with the session key Kses1, and the data decoded in step S422 are saved to the field to which memory 62 corresponds, and it uses them.

[0252] Next, although the session key which the common key module 122 shares with the reader writer 2-13 for intermodule communications differs from the session key which the public key module 121 shares with the reader writer 2-13 for intermodule communications with reference to the flow chart of drawing 50 The reader writer 2-13 for intermodule communications the session key which the common key module 122 has It enciphers with another [which the public key module 121 has] session key, and the intermodule communication in the case of being made as [supply / the public key module 121] is explained.

[0253] In step S451 thru/or step S456, the same processing as step S411 of drawing 48 thru/or step S416 is performed. That is, the session key Kses1 is shared with the inter module reader writer 2-13 between the public key modules 121, and the session key Kses2 is shared with the inter module reader writer 2-13 between the common key modules 122.

[0254] In step S457, the control section 101 of the reader writer 2-13 for intermodule communications controls the cipher-processing section 102, makes the session key Kses2 encipher with the session key Kses1, and transmits to the public key module 121. The control section 61 of the public key module 121 takes out the session key Kses2 by making the data which controlled the

common key processing section 42 of the cipher-processing section 33, and were received decode with the session key Kses1.

[0255] In step S459, the same processing as step S417 of drawing 48 is performed. In step S460, the control section 61 of the public key module 121 enciphers the data which move with the session key Kses2, and transmits encryption data to the reader writer 2-13 for intermodule communications.

[0256] In step S461, the same processing as step S440 of drawing 49 is performed. And in step S462 and step S463, the same processing as steps S422 and S423 of drawing 48 is performed.

[0257] Namely, in step S420 and step S421 of drawing 48, decode the received data with the session key Kses1, and although it transmitted to the common key module 122 after enciphering the decoded data with the session key Kses2 Here, like the processing explained using drawing 49, since the common key module 122 and the public key module 121 can obtain the same session key Kses2, it is not necessary to perform these processings.

[0258] And with reference to the flow chart of drawing 51, the public key module 121 and the common key module 122 share common private key K_common, and perform mutual recognition using it, and the intermodule communication in the case of sharing the still more common session key Kses is explained.

[0259] In step S471 and step S472, by common private key K_common, the

public key module 121 and the common key module 122 perform mutual recognition, and share the session key Kses. In step S473, the reader writer 2-13 for intermodule communications offers only the channel of the mutual recognition in step S471 and step S472 (namely, as for sharing of a session key, the public key module 121 and the common key module 122 are not performed).

[0260] In step S474, the same processing as step S417 of drawing 48 is performed. In step S475, the control section 61 of the public key module 121 makes the data which control the common key processing section 42 of the cipher-processing section 33, and move encipher with the session key Kses, and transmits encryption data to the reader writer 2-13 for intermodule communications. And in step S476 thru/or step S478, the same processing as step S421 of drawing 49 thru/or step S423 is performed.

[0261] Namely, in the intermodule communication explained using drawing 51, the reader writer 2-13 for intermodule communications does not encipher the data by which it is only offering the channel of data and intermodule communication is carried out, or does not decode them.

[0262] A series of processings mentioned above can also be performed with software. The software is that the program which constitutes the software installs the computer built into the hardware of dedication, or various kinds of programs, and is installed in a general-purpose personal computer etc. from a record

medium possible [performing various kinds of functions].

[0263] This record medium is constituted apart from a computer by the package media which are distributed in order to provide a user with a program and which consist of the magnetic disk 115 (a floppy (trademark) disk is included) with which the program is recorded, an optical disk 116 (CD-ROM (Compact Disk-Read Only Memory) and DVD (Digital Versatile Disk) are included), a magneto-optic disk 117 (MD (Mini-Disk) is included), or semiconductor memory 118, as shown in drawing 9.

[0264] Moreover, in this specification, even if the processing serially performed in accordance with the sequence that the step which describes the program recorded on a record medium was indicated is not of course necessarily processed serially, it is a juxtaposition thing also including the processing performed according to an individual.

[0265]

[Effect of the Invention] According to the data storage of this invention, a data store method, and the program currently recorded on the record medium The 1st service ID corresponding to [control I/O of the data to an information processor, control the data storage corresponding to two or more services, and] the 1st service of two or more services I/O of data is permitted when I/O of the data about the 1st service is controlled by processing of an input/output control step.

Since storage of the 2nd service ID corresponding to the 2nd service of two or more services was controlled It can make it possible to perform in parallel transfer of the data about other services permitted beforehand, securing security, when transfer of the data about predetermined service is being performed.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing for explaining the communication mode and authentication method of an IC card and a reader writer.

[Drawing 2] It is drawing for explaining the relation of a card publisher, a service provider, and a card holder.

[Drawing 3] It is the block diagram showing the configuration of an IC card.

[Drawing 4] It is the block diagram showing the configuration of an IC card.

[Drawing 5] It is drawing for explaining drawing 3 and the cipher-processing section of drawing 4 .

[Drawing 6] It is drawing for explaining SRA of drawing 3 and drawing 4 .

[Drawing 7] It is drawing for explaining the key information for authentication stored in SRA of drawing 6 .

[Drawing 8] It is drawing for explaining SRT of drawing 3 and drawing 4 .

[Drawing 9] It is the block diagram showing the configuration of a reader writer.

[Drawing 10] It is drawing for explaining the memory information on the reader writer for service registration.

[Drawing 11] It is drawing for explaining the memory information on a general reader writer.

[Drawing 12] It is drawing for explaining the memory information on the reader writer for intermodule communications.

[Drawing 13] It is drawing for explaining intermodule communication.

[Drawing 14] It is drawing for explaining the memory information on the reader writer for version up.

[Drawing 15] It is a flow chart for explaining authentication processing of an IC card and a reader writer.

[Drawing 16] It is a flow chart for explaining service discernment processing of a reader writer.

[Drawing 17] It is a flow chart for explaining service discernment processing of an IC card.

[Drawing 18] It is a flow chart for explaining service discernment processing of a reader writer.

[Drawing 19] It is a flow chart for explaining service discernment processing of

an IC card.

[Drawing 20] It is a flow chart for explaining authentication key discernment processing of a reader writer.

[Drawing 21] It is a flow chart for explaining authentication key discernment processing of an IC card.

[Drawing 22] It is a flow chart for explaining authentication key discernment processing of a reader writer.

[Drawing 23] It is a flow chart for explaining authentication key discernment processing of an IC card.

[Drawing 24] It is drawing for explaining a certificate.

[Drawing 25] It is a flow chart for explaining signature generation processing.

[Drawing 26] It is a flow chart for explaining signature verification processing.

[Drawing 27] It is a flow chart for explaining authentication key discernment processing of a reader writer.

[Drawing 28] It is a flow chart for explaining authentication key discernment processing of an IC card.

[Drawing 29] It is a flow chart for explaining service registration processing of the reader writer for service registration.

[Drawing 30] It is a flow chart for explaining service registration processing of an IC card.

[Drawing 31] It is a flow chart for explaining the service deletion of the reader writer for service registration.

[Drawing 32] It is a flow chart for explaining the service deletion of an IC card.

[Drawing 33] It is a flow chart for explaining the service deletion of a general reader writer.

[Drawing 34] It is a flow chart for explaining the service deletion of an IC card.

[Drawing 35] It is a flow chart for explaining service data acquisition processing of a general reader writer.

[Drawing 36] It is a flow chart for explaining service data transmitting processing of an IC card.

[Drawing 37] It is a flow chart for explaining service data acquisition processing of a general reader writer.

[Drawing 38] It is a flow chart for explaining service data transmitting processing of an IC card.

[Drawing 39] It is a flow chart for explaining service data write-in processing of a general reader writer.

[Drawing 40] It is a flow chart for explaining service data write-in processing of an IC card.

[Drawing 41] It is a flow chart for explaining service data write-in processing of a general reader writer.

[Drawing 42] It is a flow chart for explaining service data write-in processing of an IC card.

[Drawing 43] It is a flow chart for explaining key version up processing of the reader writer for version up.

[Drawing 44] It is a flow chart for explaining key version up processing of an IC card.

[Drawing 45] It is a flow chart for explaining key version up processing of a general reader writer.

[Drawing 46] It is a flow chart for explaining key version up processing of an IC card.

[Drawing 47] It is a flow chart for explaining key version up processing of an IC card.

[Drawing 48] It is a flow chart for explaining intermodule communication processing.

[Drawing 49] It is a flow chart for explaining intermodule communication processing.

[Drawing 50] It is a flow chart for explaining intermodule communication processing.

[Drawing 51] It is a flow chart for explaining intermodule communication processing.

[Description of Notations]

1 IC Card 1 Reader Writer 21 Communications Department 31 Control Section,
32 memory 33 Cipher-processing section 41 Public key processing section, 42
Common key processing section 43 The other cipher-processing sections 45
SRT, 46 SRA 51 Communications department 52 Common key service
processing section, 53 Communications department 54 Public key service
processing section 61 Control section, 62 Memory, 63 Cipher-processing
section 91 Communications department 101 Control section, 102
Cipher-processing section 103 Memory, the 111 public-key processing section
112 Common key processing section 113 The other cipher-processing sections
105 Display 106 Input section 121 Public key module 122 Common key module

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-357365

(P2001-357365A)

(43) 公開日 平成13年12月26日 (2001. 12. 26)

(51) Int.Cl. ⁷	識別記号	F I	テームコード* (参考)
G 0 6 K 17/00		G 0 6 K 17/00	R 5 B 0 3 5
			T 5 B 0 5 8
19/07		G 0 9 C 1/00	6 6 0 A 5 J 1 0 4
19/00		G 0 6 K 19/00	H
G 0 9 C 1/00	6 6 0		U
審査請求 未請求 請求項の数 5 O L (全 39 頁)			

(21) 出願番号 特願2000-180051 (P2000-180051)

(22) 出願日 平成12年6月15日 (2000. 6. 15)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 白井 太三

東京都品川区北品川6丁目7番35号 ソニ

ー株式会社内

(72) 発明者 石橋 義人

東京都品川区北品川6丁目7番35号 ソニ

ー株式会社内

(74) 代理人 100082131

弁理士 稲本 義雄

最終頁に続く

(54) 【発明の名称】 データ記憶装置およびデータ記憶方法、並びに記録媒体

(57) 【要約】

【課題】 1枚のICカードで、セキュリティを確保しつつ、複数のサービスの供給を同時に受けることができるようにする。

【解決手段】 Service Relation Tableには、IDカードに複数のサービスが登録されている場合に、あるサービスを行いながら別のサービスのサービスデータに対してアクセスを許可するためのデータが登録されており、ICカードに登録されているサービスIDが記載されている登録サービスIDフィールドと、それぞれのサービスIDに対応するパーミッション情報が記載されているパーミッション情報フィールドで構成されている。パーミッション情報は、対応するサービスが実行されている場合にアクセスすることができるサービスIDと、アクセス可能なサービスIDに対して、実行可能な処理を示す情報が記載されている。

Service Relation Table		パーミッション情報
登録サービスID	サービスID	
A	C (rw, vup), D (ro)	RW: Read and Write allowed RO: Read Only VUP: Key Version Up allowed
B	E (rw, vup)	
C	A (ro), B (ro), C (ro)	
D	G (ro, vup), H (rw, vup)	
E	H (rw, vup)	
F	B (rw)	
G		
H		
I		
J		

ICカード
サービスID
A, B, C, D, E
F, G, H, I, Jに対応

Service Relation Tableに登録されている情報

【特許請求の範囲】

【請求項 1】 情報処理装置に装着され、前記情報処理装置とデータの授受を行うデータ記憶装置において、前記情報処理装置に対する、前記データの入出力を制御する入出力制御手段と、

複数のサービスに対応するデータの記憶を制御する第 1 の記憶制御手段と、

前記複数のサービスのうちの第 1 のサービスに対応する第 1 のサービス ID と、前記入出力制御手段により前記第 1 のサービスに関する前記データの入出力が制御されている場合に前記データの入出力が許可される、前記複数のサービスのうちの第 2 のサービスに対応する第 2 のサービス ID の記憶を制御する第 2 の記憶制御手段とを備えることを特徴とするデータ記憶装置。

【請求項 2】 前記第 2 の記憶制御手段は、前記第 2 のサービスに関するアクセス権の制限に関する情報の記憶をさらに制御することを特徴とする請求項 1 に記載のデータ記憶装置。

【請求項 3】 前記第 2 の記憶制御手段は、前記第 2 のサービス ID が、前記第 1 のサービス ID に対して複数存在する場合、複数の前記第 2 のサービス ID の記憶を制御し、前記第 2 のサービス ID が、前記第 1 のサービス ID に対して 1 つも存在しない場合、前記第 2 のサービス ID が空欄となるように記憶を制御することを特徴とする請求項 1 に記載のデータ記憶装置。

【請求項 4】 情報処理装置に装着され、前記情報処理装置とデータの授受を行うデータ記憶装置のデータ記憶方法において、

前記情報処理装置に対する、前記データの入出力を制御する入出力制御ステップと、

複数のサービスに対応するデータの記憶を制御する第 1 の記憶制御ステップと、

前記複数のサービスのうちの第 1 のサービスに対応する第 1 のサービス ID と、前記入出力制御ステップの処理により前記第 1 のサービスに関する前記データの入出力が制御されている場合に前記データの入出力が許可される、前記複数のサービスのうちの第 2 のサービスに対応する第 2 のサービス ID の記憶を制御する第 2 の記憶制御ステップとを含むことを特徴とするデータ記憶方法。

【請求項 5】 情報処理装置に装着され、前記情報処理装置とデータの授受を行うデータ記憶装置用のプログラムであって、

前記情報処理装置に対する、前記データの入出力を制御する入出力制御ステップと、

複数のサービスに対応するデータの記憶を制御する第 1 の記憶制御ステップと、

前記複数のサービスのうちの第 1 のサービスに対応する第 1 のサービス ID と、前記入出力制御ステップの処理により前記第 1 のサービスに関する前記データの入出力

が制御されている場合に前記データの入出力が許可される、前記複数のサービスのうちの第 2 のサービスに対応する第 2 のサービス ID の記憶を制御する第 2 の記憶制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、データ記憶装置およびデータ記憶方法に関し、例えば、IC カードと、リーダライタとが、所定のサービスに関するデータの授受を実行している場合において、セキュリティを確保しつつ、予め許可された他のサービスに関するデータの授受を、並行して行うことを可能とするデータ記憶装置およびデータ記憶方法に関する。

【0002】

【従来の技術】電子マネーシステムや、セキュリティシステムにおいて、IC (Integrated circuit) カードの利用が増加している。IC カードは、各種処理を行う CPU (Central Processing Unit) や、処理に必要なデータなどを記憶するメモリを内蔵しており、所定のリーダライタに電氣的に接触させた状態で、または電磁波を利用して非接触で、データの送受信が行われる。なお、リーダライタとの間で、電磁波を利用して非接触でデータの送受信を行う IC カードには、一般に、その電磁波により、必要な電力が供給される。

【0003】IC カードと、リーダライタの認証には、共通鍵方式もしくは公開鍵方式が用いられる。共通鍵方式では、暗号化に使用する鍵と、復号に使用する鍵が同じである。共通鍵暗号を使うには、前もって送信者と受信者の間で共通鍵を共有する必要があるため、暗号化に使用した鍵を、通信路とは別の安全な手段を使って、通信相手に届けておく必要がある（すなわち、IC カードとリーダライタが共通鍵を予め共有していなければならない）。暗号化は、基本的には、文字の順序を入れ換える「転置（転字）」と、一定の規則に従ってある文字を別の文字に置き換える「換字」を組み合わせて行われる。どのような順序で入れ換えるか、どの文字とどの文字が置き換えてあるかを示すのが暗号アルゴリズムと鍵である。暗号化において、文字をずらすための換字暗号や文字の順序を変えるための転置暗号が基本的な暗号変換であり、ずらされる文字数などが鍵となる。

【0004】公開鍵方式は、暗号システムにおいて、「暗号化鍵」と「復号鍵」という 2 つの鍵をペアで使い、そのうちの暗号化鍵は公開し、復号鍵は、鍵の発行者が管理して秘密にしておくものである。データを送信する場合は、暗号化鍵を使って通信文を暗号化し、受信した側では復号鍵を使って元に戻す。2 つの鍵はある数学的な関係に基づいて決められているので、暗号化鍵から復号鍵を求めるのは不可能ではないが、計算量の点から現実的ではない。

【0005】公開鍵暗号システムは、従来の共通鍵暗号システムに比べて、暗号化鍵は秘匿する必要がないので、暗号化鍵の配布が容易であり、暗号文を復号するには、各ユーザが個々に持っている復号鍵さえあればよいので、復号鍵を配布する必要がなく、更に、デジタル署名によるメッセージの認証機能を持つ、という利点を有するが、共通鍵暗号システムに比べて、認証処理にかかる時間が長くなる。

【0006】デジタル署名とは、電子メールやオンライン取り引きなどにおいて、そのメッセージが正当な発信者から発信され、途中で改ざんなどが行なわれていないことを示すための方法である。通常の暗号文通信では、公開鍵で暗号化を行うが、例えば、RSA (Rivest, Shamir, Adleman) 公開鍵暗号システムの場合には、逆に、「復号鍵(秘密鍵)で暗号化を行う」とデジタル署名となる。また、他の暗号方式では、署名を付加したいデータに対して、ハッシュ値を取り、それを秘密鍵で暗号化している。

【0007】この署名を検証するには、公開鍵が用いられる(すなわち、暗号化鍵と復号鍵の役割が入れ換えられる)。公開鍵は広く公開されているので、だれでもその署名の正当性を簡単に検査することができる。もし公開鍵で暗号文を正しく復元することができ、意味のある文が得られれば、それは正しい発信者であると確認することができる。なぜなら、秘密鍵(署名を行った鍵)を知っているのは正規の発信者だけであり、公開鍵で復元できるようなデジタル署名を作成するには、そのペアとなる秘密鍵を知らなければいけないからである。また、データが改ざんされた場合、データは正しく復元することができなくなるため、改ざんの防止・検出にも利用することができる。署名の検証は、公開鍵を用いて復号した値と、別途、データから計算しなおしたハッシュ値とを比較することにより実行され、一致していれば、データは改ざんされていないと判断され、一致していなければ、データの改ざんが行われたと判断される。

【0008】また、データの発行元が信頼のおける組織であることを証明するための証明書を発行することを目的とした第三者の組織を、認証局(CA (Certificate Authority))という。

【0009】

【発明が解決しようとする課題】従来、ICカードを用いて複数のサービスを受ける場合、1つのサービスを受けている間は、他のサービスを受けることができない。なぜならば、ICカードとリーダライタにおいて、所定のデータを授受するためには、それぞれのデータに対するセキュリティを確保するために、認証処理を行う必要があるからである。しかしながら、例えば、同一のICカードと同一のリーダライタを用いて、プリペイドサービスと電子マネーサービスを受けることができるような場合、プリペイドサービスに関する清算処理を行いな

ら、電子マネーの充填を行いたいという要求がある。

【0010】本発明はこのような状況に鑑みてなされたものであり、所定のサービスに関するデータの授受を実行している場合において、セキュリティを確保しつつ、予め許可された他のサービスに関するデータの授受を、並行して行うことを可能とするものである。

【0011】

【課題を解決するための手段】本発明のデータ記憶装置は、情報処理装置に対する、データの入出力を制御する入出力制御手段と、複数のサービスに対応するデータの記憶を制御する第1の記憶制御手段と、複数のサービスのうちの第1のサービスに対応する第1のサービスIDと、入出力制御手段により第1のサービスに関するデータの入出力が制御されている場合にデータの入出力が許可される、複数のサービスのうちの第2のサービスに対応する第2のサービスIDの記憶を制御する第2の記憶制御手段とを備えることを特徴とする。

【0012】第2の記憶制御手段には、第2のサービスに関するアクセス権の制限に関する情報の記憶を制御させることができる。

【0013】第2の記憶制御手段には、第2のサービスIDが、第1のサービスIDに対して複数存在する場合、複数の第2のサービスIDの記憶を制御させ、第2のサービスIDが、第1のサービスIDに対して1つも存在しない場合、第2のサービスIDが空欄となるように記憶を制御させることができる。

【0014】本発明のデータ記憶方法は、情報処理装置に対する、データの入出力を制御する入出力制御ステップと、複数のサービスに対応するデータの記憶を制御する第1の記憶制御ステップと、複数のサービスのうちの第1のサービスに対応する第1のサービスIDと、入出力制御ステップの処理により第1のサービスに関するデータの入出力が制御されている場合にデータの入出力が許可される、複数のサービスのうちの第2のサービスに対応する第2のサービスIDの記憶を制御する第2の記憶制御ステップとを含むことを特徴とする。

【0015】本発明の記録媒体に記録されているプログラムは、情報処理装置に対する、データの入出力を制御する入出力制御ステップと、複数のサービスに対応するデータの記憶を制御する第1の記憶制御ステップと、複数のサービスのうちの第1のサービスに対応する第1のサービスIDと、入出力制御ステップの処理により第1のサービスに関するデータの入出力が制御されている場合にデータの入出力が許可される、複数のサービスのうちの第2のサービスに対応する第2のサービスIDの記憶を制御する第2の記憶制御ステップとを含むことを特徴とする。

【0016】本発明のデータ記憶装置、データ記憶方法および記録媒体に記録されているプログラムにおいては、情報処理装置に対するデータの入出力が制御され、

複数のサービスに対応するデータの記憶が制御され、複数のサービスのうちの第1のサービスに対応する第1のサービスIDと、入出力制御ステップの処理により第1のサービスに関するデータの入出力が制御されている場合にデータの出入力が許可される、複数のサービスのうちの第2のサービスに対応する第2のサービスIDの記憶が制御される。

【0017】

【発明の実施の形態】以下、図を参照して、本発明の実施の形態について説明する。

【0018】図1に、ICカードとリーダライタの関係を示す。ICカード1は、共通鍵方式による認証と、公開鍵方式による認証の両方の認証サービスに対応することが可能である（それぞれの認証方法については後述する）。非接触式共通鍵対応リーダライタ2-1は、ICカード1と非接触で通信を行い、共通鍵方式で認証を行う。非接触式公開鍵対応リーダライタ2-2は、ICカード1と非接触で通信を行い、公開鍵方式で認証を行う。接触式公開鍵対応リーダライタ2-3は、接触して通信を行い、公開鍵方式で通信を行う。

【0019】例えば、ICカード1に定期券や運賃の支払いを行うことができるプリペイドカードなどのサービスを提供する情報が含まれており、ICカード1を用いて駅の改札を利用する場合や、ICカード1に、IDカードとしての機能が含まれており、ICカード1を用いて入室許可の認証を行う場合などの、短い処理時間が求められる処理においては、非接触式共通鍵対応リーダライタ2-1を用いて、共通鍵による非接触の通信が行われる。

【0020】例えば、ICカード1に、電子マネーのサービスを提供する情報が含まれており、店舗などでユーザが購買した商品の清算の処理を行う場合などは、公開鍵方式により認証が行われ、認証処理に時間がかかる。このため、処理時間を特に気にしないような場合は、非接触式公開鍵対応リーダライタ2-2を用いて、非接触で通信を行ってもよいし、処理時間を短縮するために、接触式公開鍵対応リーダライタ2-3を用いて、接触して通信を行うようにしてもよい。

【0021】図1においては、非接触式共通鍵対応リーダライタ2-1乃至接触式公開鍵対応リーダライタ2-3を、個別のリーダライタとして説明しているが、必要に応じて、1つのリーダライタで、複数の通信方法や複数の認証方法を用いることができるようにしてもよい。

【0022】次に、図2を用いて、カード発行者、サービス提供者、およびカード保持者について説明する。

【0023】カード発行者11は、サービス提供者12に、ICカード1を保有するカード保持者13に対して、ICカード1を用いたサービスの提供を行うことを認可し、ICカード1の発行を希望したカード保持者13に対して、ICカード1を発行する。

【0024】カード発行者11から、サービスの認可を受けたサービス提供者12は、カード発行者11が有するサービス登録用リーダライタ2-1に、自分自身がカード保持者13に提供するサービスに対応するデータ（図6を用いて後述するService Individual Info）を登録する。この登録については、例えば、サービス提供者12が有する図示しないパーソナルコンピュータなどから、インターネットなどを介して、サービス登録用リーダライタ2-1に登録するようにしてもよいし、オペレータが手動で登録するようにしてもよい。

【0025】カード保持者13は、サービス登録用リーダライタ2-1を用いて、カード発行者11から発行されたICカード1に、希望するサービスを登録させることができる。サービス登録用リーダライタ2-1と、ICカード1のサービス登録処理については、図29および図30を用いて後述する。

【0026】そして、カード保持者13は、自分自身のICカード1に登録されているサービスの削除を行いたい場合、カード発行者11が管理するサービス登録用リーダライタ2-11、もしくは、サービス提供者12が管理する一般リーダライタ2-12を用いて、自分自身のICカード1から、サービスを削除させることができる。ICカード1とサービス登録用リーダライタ2-11のサービス削除処理については、図31および図32、ICカード1と一般リーダライタ2-12のサービス削除処理については、図33および図34を用いて後述する。

【0027】また、カード保持者13は、例えば、ICカード1に、電子マネーサービスとプリペイドサービスが登録されており、それぞれの価値情報が、ICカード1のそれぞれのサービスに関する情報に記録されている状況で、電子マネーの価値の一部を、プリペイドの価値へ置き換えたい場合、サービス提供者12が管理するモジュール間通信用リーダライタ2-13を用いて、自分自身のICカード1の、図13を用いて後述する公開鍵モジュールと共通鍵モジュールの間で、モジュール間通信を実行させることができる。モジュール間通信用リーダライタ2-13は、共通鍵方式と、公開鍵方式の2方式に対応するようになされている。ICカード1とモジュール間通信用リーダライタ2-13との処理については、図48乃至図51を用いて後述する。

【0028】更に、カード保持者13は、失効してしまった認証鍵の更新（バージョンアップ）を行いたい場合、サービス提供者12が管理する一般リーダライタ2-12、もしくは、バージョンアップ用リーダライタ2-14を用いて、自分自身のICカード1に登録されている認証鍵のバージョンアップを行わせることができる。ICカード1とバージョンアップ用リーダライタ2-14との鍵バージョンアップ処理については、図43および図44を用いて、ICカード1と一般リーダライタ

2-12との鍵バージョンアップ処理については、図45乃至47を用いて後述する。

【0029】図3は、ICカード1の構成を示すブロック図である。

【0030】ICカード1は、リーダライタ2（リーダライタ2-1乃至2-3、もしくはリーダライタ2-1乃至2-14を特に区別する必要のない場合については、これらを総称して、リーダライタ2と称するものとする）との通信を行う通信部21と、データ処理を実行するICカード処理部22から構成されている。

【0031】通信部21は、対応するICカード1が、図1を用いて説明した非接触式共通鍵対応リーダライタ2-1、もしくは非接触式公開鍵対応リーダライタ2-2である場合、非接触式共通鍵対応リーダライタ2-1、もしくは非接触式公開鍵対応リーダライタ2-2と、電磁波を用いて通信するためのコイルを備えている。また、通信部21は、ICカード1が、図1を用いて説明した非接触式共通鍵対応リーダライタ2-1、および非接触式公開鍵対応リーダライタ2-2のみならず、接触式公開鍵対応リーダライタ2-3との通信にも対応している場合、非接触式共通鍵対応リーダライタ2-1、もしくは非接触式公開鍵対応リーダライタ2-2と、電磁波を用いて通信するためのコイルと、接触式公開鍵対応リーダライタ2-3と通信するための接触端子を備えている。

【0032】通信部21は、リーダライタ2から送信されたデータを受信し、受信したデータが、例えば、ASK（Amplitude Shift Keying）やBPSK（Binary Phase Shift Keying）を用いて変調されている場合、所定の処理により、受信したデータを復調し、ICカード処理部22の制御部31に供給するとともに、ICカード処理部22の処理により生成されたデータを、制御部31から供給され、ASKやBPSKを用いて変調し、リーダライタ2に送信する。

【0033】ICカード処理部22は、制御部31、メモリ32、および暗号処理部33より構成されている。制御部31は、通信部21から供給されたデータに従って、暗号処理部33を制御し、リーダライタ2との認証処理等に必要な暗号処理を実行させたり、必要に応じて、メモリ32に記録されているデータを読み込んで、通信部21を介して、リーダライタ2に送信する。

【0034】メモリ32は、カードID、サービス登録用の認証鍵Kreg、認証局の公開鍵であるCA_Pubが記録されているメモリ領域44、図8を用いて後述するService Relation Table（SRT）45、および図6を用いて後述するService Registration Area（SRA）46で構成されている。

【0035】暗号処理部33は、公開鍵処理部41、共通鍵処理部42、その他の暗号処理部43で構成されている。公開鍵処理部41乃至その他の暗号処理部43が

実行する処理に関する詳細は、図5を用いて後述する。

【0036】次に、図4は、ICカード1の、図3と異なる構成を示すブロック図である。なお、図4のICカード1においては、図3における場合と対応する部分には同一の符号を付してあり、その説明は適宜省略する（以下、同様）。

【0037】ICカード1は、共通鍵サービスに関するリーダライタ2との通信を実行する通信部51、通信部51の処理によって得られたデータの処理を実行する共通鍵サービス処理部52、公開鍵サービスに関するリーダライタ2との通信を実行する通信部53、通信部53の処理によって得られたデータの処理を実行する公開鍵サービス処理部54から構成されている。

【0038】通信部51は、非接触式共通鍵対応リーダライタ2-1と通信を行うためのコイルを備えており、通信部21と同様に、例えば、ICカード1から送信されるデータが、ASKやBPSKを用いて変調されている場合、所定の処理により、受信したデータを復調し、共通鍵サービス処理部52の制御部61に供給するとともに、共通鍵サービス処理部52の処理により生成されたデータを、制御部61から供給され、ASKやBPSKを用いて変調し、リーダライタ2に送信する。

【0039】共通鍵サービス処理部52は、制御部61、メモリ62、および暗号処理部63から構成されている。制御部61は、通信部51から供給されたデータに従って、暗号処理部63を制御し、ICカード1との認証処理等に必要な処理を実行させたり、必要に応じて、メモリ62に記録されているデータを読み込んで、通信部51を介して、リーダライタ2に送信する。

【0040】メモリ62は、図3を用いて説明したメモリ32と同様に、メモリ領域44、SRT45、およびSRA46で構成されている。メモリ領域44には、カードID、サービス登録用の認証鍵Kreg、および、モジュール間通信で用いられる共有秘密鍵K_commonが記録されている。

【0041】暗号処理部63は、共通鍵処理部42、その他の暗号処理部43で構成されている。すなわち、共通鍵サービス処理部52においては、公開鍵に関するサービスを処理しないため、暗号処理部63には、図3を用いて説明した公開鍵処理部41は備えられていない。

【0042】通信部53は、非接触式公開鍵対応リーダライタ2-2、あるいは、接触式公開鍵対応リーダライタ2-3と通信を行うためのコイルもしくは接触端子を備えている。通信部53も、通信部21と同様に、例えば、ICカード1から送信されるデータが、ASKやBPSKを用いて変調されている場合、所定の処理により、受信したデータを復調し、公開鍵サービス処理部54の制御部61に供給するとともに、公開鍵サービス処理部54の処理により生成されたデータを、制御部61から供給され、ASKやBPSKを用いて変調し、リー

ドライタ2に送信する。

【0043】公開鍵サービス処理部54は、制御部61、メモリ62、および暗号処理部33から構成されている。すなわち、暗号処理部63に代わって、図3を用いて説明した暗号処理部33が備えられている以外は、共通鍵サービス処理部と、基本的に同様の構成である。

【0044】次に、図5を用いて、公開鍵処理部41乃至その他の暗号処理部43について説明する。

【0045】図5(A)に示されるように、公開鍵処理部41には、例えば、RSA (Rivest, Shamir, Adleman) 公開鍵暗号システムを利用して署名の生成および検証を行うRSA署名生成・検証部71や、DSA (Digital Signature Algorithm) 方式を利用して署名の生成および検証を行うDSA署名生成・検証部72が備えられている。

【0046】RSA署名生成・検証部71では、2つの鍵によって暗号化と復号を行う。RSA暗号系では、2つの鍵は、例えば、次のようにして決められる。

【0047】ある2つの大きな素数 p と q を選んで、その積 $n=pq$ を求める。そして、 $(p-1) \times (q-1)$ 以下で $(p-1) \times (q-1)$ と互いに素な整数 e を選び、次の式 (1) を満たす整数 d を求める。

$$E \times d = 1 \bmod ((p-1) \times (q-1)) \cdots (1)$$

すると、 (e, n) が公開鍵、 d が秘密鍵となる。

【0048】文 M を暗号化して、暗号化データ C を生成する場合、次の式 (2) を用いる。

$$C = M^e \bmod n \cdots (2)$$

また、暗号化データ C を復号する場合、次の式 (3) を用いる。

$$M = C^d \bmod n \cdots (3)$$

【0049】DSA署名生成・検証部72には、図示しない乱数生成部が備えられている。DSAは、DLP (Discrete Logarithm Problem: 離散対数問題) の困難性をベースとしたElGamal署名を改良して、署名の長さを160bit $\times 2$ に短縮し、署名鍵の生成等を特定の方法で運用するデジタル署名アルゴリズムである。署名生成において、ハッシュ関数 (データ圧縮関数) にSHA-1 (Secure Hash Algorithm-1) を使うことを前提としている。DSA方式は、米国政府機関であるNIST (米国商務省標準技術局: National Institute of Standards and Technology) により、電子署名の標準として開発され、米国連邦情報処理標準 (Federal Information Processing Standard) FIPS PUB 186に定められた。

【0050】また、図5(B)に示されるように、共通鍵処理部42には、例えば、DES (Data Encryption Standard) 共通鍵暗号システムによる認証処理を行うDES処理部73、RC5 (Rivest Cipher 5) 方式による認証処理を行うRC5処理部74、およびAES (Advanced Encryption Standard) 方式による認証処理を行うAES処理部75が備えられている。

【0051】DES共通鍵暗号システムは、1977年にNISTで制定され、1981年に米国規格協会 (ANSI: American National Standards Institute) により標準化された共通鍵暗号システムである。DES共通鍵暗号システムの鍵の認証アルゴリズムは公開されており、共通鍵暗号システムの代表として広く普及している。

【0052】DES共通鍵暗号システムは、データを64bit単位に区切って暗号化および復号処理を行う暗号システムである。DESアルゴリズムにおいては、暗号化と復号は対称をなしており、受信した暗号文を同じ鍵を使ってもう一度変換すれば元の文章が復元できる。また、DES共通鍵暗号システムでは、簡単なビット位置転置とXOR演算の組み合わせ論理を16回繰り返している。内部的にはデータのフィードバックや条件判断部分がなく、処理が逐次的なので、パイプライン化すれば高速に処理することができる。もともとLSI化することを前提にして決められたアルゴリズムであり、DESチップも多く作られている。

【0053】RC5とは、RSA Data Security社と、マサチューセッツ工科大学が開発したRCシリーズの共通鍵暗号方式であり、1995年に提案された。RC5は、可変長ブロックサイズ、可変長の鍵サイズ、および可変長回数 (元データや鍵によって、ビット回転の量が変わる、Data dependent rotations (データ依存ビット回転) アルゴリズム) のラウンドを有するブロック暗号化方式である。そのブロックサイズとしては、32、64、128ビットをとることが可能であり、ラウンド数は0から255、鍵サイズは0から2048ビットまで可変である。RC5のアルゴリズムは公開されていて、RFC2040として入手することが可能である。

【0054】また、AES方式は、NISTによって選定作業が行われている、米国政府の次世代標準暗号化方式である。現在標準暗号として用いられているDESが制定されたのは1977年であり、近年のコンピュータの高性能化、暗号理論の発展に伴い、その信頼性は年々低下している。そこで、NISTはDESに代わる次世代の暗号標準として、AES候補となる暗号方式を全世界から公募した。世界中から集まった15の方式が審査を受けており、21世紀初頭までに決定される予定である。

【0055】そして、その他の暗号処理部43は、例えば、デジタル署名を用いる場合に、メッセージに対して、不可逆的なハッシュ関数を作用させることで、「メッセージダイジェスト」を作成し、メッセージダイジェストを署名鍵により暗号化することによって、デジタル署名を作成する等の、公開鍵処理部41もしくは共通鍵処理部42が処理する以外の暗号処理を実行する。その他の暗号処理部43には、図5(C)に示されるように、例えば、署名生成および署名検証に用いられるハッシュ関数SHA-1の処理を行うSHA-1処理部76、および相互認証プロトコルで利用される真性乱数を生成する真性

乱数生成部77が備えられるか、あるいは、図5(D)に示されるように、署名生成および署名検証に用いられるハッシュ関数MD5の処理を行うMD5処理部78、および相互認証プロトコルで利用される擬似乱数(ある有限な桁数の数字の範囲で出来るだけランダムな数字列をもつ人工的な乱数)を生成する擬似乱数生成部79が備えられている。

【0056】デジタル署名においては、公開鍵暗号方式を用いるため、処理速度が遅いことが問題となるが、メッセージダイジェストを作成することによって、デジタル署名作成にかかる時間が削減される。更に、ハッシュ関数は、データの改ざんに対して大きく反応する特性を有していることから、デジタル署名を検証する際に、デジタル署名を検証鍵で復号して取り出したメッセージダイジェストと、送られてきたメッセージ本文にハッシュ関数を作用させて作成したメッセージダイジェストを比較することにより、メッセージ本文が改ざんされていないかどうかを容易に確認することができる。

【0057】SHA-1は任意の長さのメッセージから160bitのハッシュ値を生成する一方ハッシュ関数である。DSA同様、NISTが開発したもので、NISTによってFIPS PUB180に定められた。標準原案(N544)は、基本的にFIPS PUB 180に準拠したものとなっている。

【0058】そして、MD5は、広く一般に使われているメッセージダイジェスト関数アルゴリズムのうちの1つで、RFC1321で定義されている。MD5は、32bitコンピュータ上で効率よく計算できるように、アルゴリズムが決められている。ほかにMD4やMD2という、類似のアルゴリズムもある。

【0059】次に、図6を用いて、図3および図4を用いて説明したICカード1のSRA46に格納されている情報について説明する。

【0060】SRA46は、ICカード1を保有するユーザが、図2を用いて説明した一般リーダライタ2-12などを用いて、複数のサービスを受けることができるようにするために、それらの複数のサービスを受けるための情報(図2を用いて説明したサービス登録用リーダライタ2-11を用いて登録された情報)を記録するためのメモリ領域である。

【0061】すなわち、SRA46には、そのICカード1に登録されているサービスの情報であるService Individual Info1乃至Nが登録されており、それぞれのService Individual Infoには、サービスの種類を識別するためのサービスID、サービス毎に予め定められた、1つ、もしくは複数の認証用鍵情報(図6におけるService Individual Info kにおいては、1乃至nのn個の認証用鍵情報)、サービスを受けるために利用されるサービスデータ、および、鍵情報をバージョンアップするための認証鍵ake_vupと、必要に応じて、認証鍵に対する証明書などが登録されている。

【0062】認証用鍵情報には、例えば、認証鍵ID、鍵のレベルおよびバージョン、認証方式、および、複数の認証鍵を識別するために用いられる識別用認証鍵ake(必要に応じて、認証鍵に対する証明書)などが含まれる。また、サービスデータには、ユーザID以外に、Service Individual Info kが、例えば、電子マネーサービスである場合、電子マネーの残高情報や累積ポイント等、Service Individual Info kが、例えば、自動改札サービスである場合、有効区間情報等が格納される。

【0063】次に、図7を用いて、図6のService Individual Infoに登録される認証用鍵情報について説明する。

【0064】図7(A)においては、領域No. 1および領域No. 2のそれぞれに対応して、認証鍵ID、鍵のバージョン、認証方式、識別用認証鍵ake、および、必要に応じて、証明書データが登録されている。図7(A)のように認証用鍵情報が登録されている場合の認証鍵識別処理については、図20乃至図24を用いて後述する。

【0065】図7(B)においては、領域No. 1乃至領域No. 7のそれぞれに対応して、認証鍵ID、鍵のレベル、鍵のバージョン、認証方式、識別用認証鍵ake、および、必要に応じて、証明書データが登録されている。図7(B)のように、鍵のレベルを含んだ認証用鍵情報が登録されている場合の認証鍵識別処理については、図27および図28を用いて後述する。

【0066】次に、図8を用いて、図3および図4を用いて説明したICカード1のSRT45に格納されている情報について説明する。

【0067】SRT45には、ICカード1に複数のサービスが登録されている場合に、あるサービスを行いながら別のサービスのサービスデータに対してアクセスを許可するためのデータが登録されている。SRT45は、ICカード1に登録されているサービスIDが記載されている登録サービスIDフィールド(図8においては、サービスIDA乃至Jとして記載されている)と、それぞれのサービスIDに対応するパーミッション情報が記載されているパーミッション情報フィールドで構成されている。

【0068】パーミッション情報の登録サービスIDフィールドには、登録されているサービスのサービスIDがすべて列挙されている。そして、パーミッション情報フィールドには、対応するサービスが実行されている場合に、登録サービスIDフィールドに記載されているサービスにアクセスすることができるサービスIDと、どのような処理を行うことを許可するかを示す情報が記載されている。例えば、読み出しおよび書き込みが許可されている場合、パーミッション情報として「rw」が記載され、読み出しのみ許可されている場合、パーミッション情報として「ro」が記載され、鍵のバージョンア

ップが許可されている場合、パーミッション情報として「vup」が記載される。「rw」と「ro」は同じサービスIDに対して許可されないが、「rw」と「vup」および「ro」と「vup」は、同じサービスIDに対して許可され、パーミッション情報フィールドに列挙することが可能である。

【0069】すなわち、SRT45に、図8に示されるパーミッション情報が登録されている場合、サービスIDがCで示されるサービスの実行中には、サービスIDがBで示されるサービスに対して、読み出し、および書き込みが許可され、更に、サービスIDがDで示されるサービスの実行中においても、サービスIDがBで示されるサービスに対しての読み出しが許可され、サービスIDがEで示されるサービスの実行中に、サービスIDがDで示されるサービスに対して、読み出し、書き込み、および鍵のバージョンアップが許可され、以下、サービスIDがEで示されるサービス、サービスIDがFで示されるサービス、サービスIDがGで示されるサービス、もしくは、サービスIDがIで示されるサービスにおいても、対応するパーミッション情報フィールドに記載されている情報に基づいて、他のサービスIDに対応する処理の実行中に、パーミッション情報に対応した処理が許可される。

【0070】これらのパーミッション情報の登録は、ICカード1に、対応するサービスを登録する場合に行われる。すなわち、ユーザが、サービス登録用リーダライタ2-11を用いて、自分自身が保有するICカード1に対して、サービスIDがFで示されるサービスを登録する場合、例えば、サービスIDがGで示されるサービスがすでに登録され、サービスIDがHで示されるサービスが登録されていないならば、登録サービスIDフィールドのFに対応するパーミッション情報フィールドには、サービスIDがGで示されるサービスに対応するパーミッション情報しか登録することができない。そして、ユーザが、サービスIDがHで示されるサービスをICカード1に登録した後、サービスIDがFで示されるサービスをアップデートすることにより、サービスIDがFで示されるサービスに対する、サービスIDがHで示されるサービスのパーミッション情報を登録することができる。

【0071】次に、図9は、リーダライタ2の構成を示すブロック図である。

【0072】リーダライタ2は、ICカード1との通信を行う通信部91と、データ処理を実行するリーダライタ処理部92から構成されている。

【0073】通信部91は、ICカード1との通信方法によって（すなわち、リーダライタ2が、図1を用いて説明した非接触式と接触式のいずれの通信方式を採用しているかによって）、電磁波を用いて通信するためのコイルのみを備えるか、もしくは、電磁波を用いて通信す

るためのコイル、および接触式により通信するための接触端子を備える構造を有している。

【0074】通信部91は、ICカード1から送信されたデータを受信し、受信したデータが、例えば、ASKやBPSKを用いて変調されている場合、所定の処理により、受信したデータを復調し、リーダライタ処理部92の制御部101に供給するとともに、リーダライタ処理部92の処理により生成されたデータを、制御部101から供給され、ASKやBPSKを用いて変調し、ICカード1に送信する。

【0075】リーダライタ処理部92は、制御部101、暗号処理部102、メモリ103、通信部104、表示部105、および入力部106より構成されている。制御部101は、通信部91から供給されたデータに従って、暗号処理部102を制御し、ICカード1との認証処理等に必要な暗号処理を実行させたり、必要に応じて、メモリ103に記録されているデータを読み込んで、通信部91を介して、ICカード1に送信したり、ユーザが入力部106を用いて入力した各種操作に対応した信号や、ネットワークを介して、通信部104に入力された制御信号の入力を受け、これらの信号に従って、処理を実行し、その結果を表示部105に表示させる。

【0076】また、通信部104には、ドライブ114も接続されており、ドライブ114に装着される磁気ディスク115、光ディスク116、光磁気ディスク117、および半導体メモリ118などとデータの授受を行うことができる。

【0077】暗号処理部102は、図3を用いて説明した暗号処理部33と同様の構成を有しているため、その説明は省略する。

【0078】メモリ103には、ICカード1と所定の処理を実行するための情報が記憶されている。その情報は、リーダライタ2が、図2を用いて説明した、サービス登録用リーダライタ2-11乃至バージョンアップ用リーダライタ2-14のいずれに対応するものであるかによって異なる。図10乃至図14を用いて、サービス登録用リーダライタ2-11乃至バージョンアップ用リーダライタ2-14のメモリ103に記憶されているデータについて説明する。

【0079】図10に示される、サービス登録用リーダライタ2-11のメモリ103には、ICカード1のメモリ32のSRA46にデータを登録もしくは削除する場合に用いられる認証鍵Kregが記憶され（必要に応じて認証鍵の証明書も記憶されている）、ICカード1に登録するための各種サービスに対応するService Individual Info1乃至nが記憶されている。

【0080】図11に示される、一般リーダライタ2-12のメモリ103には、この一般リーダライタ2-12で処理することが可能なサービスに対応するサービス

IDと、それに対応する認証鍵リスト、および鍵失効情報が記憶されている。また、一般リーダライタ2-12に、鍵バージョンアップのサービスを可能とさせる場合、一般リーダライタ2-12のメモリ103には、新バージョンの鍵などの情報も、あわせて記憶される。

【0081】図12に示される、モジュール間通信用リーダライタ2-13のメモリ103には、一般リーダライタ2-12のメモリ103に記憶されている情報と同様に、このモジュール間通信用リーダライタ2-13で処理することが可能なサービスに対応するサービスIDと、それに対応する認証鍵リスト、および鍵失効情報が記憶されている。モジュール間通信とは、図13に示されるように、共通鍵方式および公開鍵方式の2方式に対応するようになされているモジュール間通信用リーダライタ2-13に、公開鍵モジュール121（例えば、図4を用いて説明した、ICカード1の通信部53および公開鍵サービス処理部54に対応する）と、共通鍵モジュール122（例えば、図4を用いて説明したICカード1の通信部51および共通鍵サービス処理部52に対応する）を有するICカード1を装着し、公開鍵モジュール121と共通鍵モジュール122とのデータの通信を、モジュール間通信用リーダライタ2-13を介して行うことである。モジュール間通信に関する処理の詳細は、図48乃至図51を用いて後述する。

【0082】そして、図14に示される、バージョンアップ用リーダライタ2-14のメモリ103には、装着されたICカード1に登録されているサービスの認証鍵をバージョンアップするための、サービスIDと、そのサービスIDに対応するバージョンアップ用認証鍵 K_{ake_vup} および認証鍵 K_{ake} のリストが記憶されている。

【0083】ICカード1とリーダライタ2とが通信を行う場合、いくつかの例外となる処理を除いて、はじめに、ICカード1とリーダライタ2が相互認証するために、通信を行うサービスを相互に識別し、そのサービスの認証鍵を相互に識別する必要がある。図15のフローチャートを参照して、ICカード1とリーダライタ2の相互認証処理について説明する。

【0084】まず、ステップS1において、リーダライタ2は、必要に応じて、ICカード1と通信して必要なデータの授受を行うことにより、図16および図18を用いて後述するリーダライタ2のサービス識別処理を実行する。そして、ステップS2において、ICカード1は、必要に応じて、リーダライタ2と通信して必要なデータの授受を行うことにより、図17および図19を用いて後述するICカード1のサービス識別処理を実行する。

【0085】そして、ステップS1のリーダライタ2のサービス識別処理およびステップS2のICカード1のサービス識別処理が正常終了した場合、ステップS3において、リーダライタ2は、必要に応じて、ICカード

1と通信して必要なデータの授受を行うことにより、図20、図22および図27を用いて後述するリーダライタ2の認証鍵識別処理を実行する。そして、ステップS4において、ICカード1は、必要に応じて、リーダライタ2と通信して必要なデータの授受を行うことにより、図21、図23および図28を用いて後述するICカード1の認証鍵識別処理を実行する。

【0086】次に、図16のフローチャートを参照して、複数のサービスに対応しているICカード1と、複数のサービスに対応しているリーダライタ2において、ユーザが所望のサービスを入力し、そのサービスの実行が可能か否かを判断することにより、図15のステップS1において実行されるリーダライタ2のサービス識別処理について説明する。

【0087】リーダライタ2の制御部101は、ステップS11において、ICカード1に対し、通信部91を介して、ICカード検出コマンドを送信し、ステップS12において、ICカード1からACK信号（後述する図17のステップS22において、ICカード1が送信した信号）を受信したか否かを判断する。ステップS12において、ACK信号が受信されていないと判断された場合、ACK信号が受信されたと判断されるまで、ステップS12の処理が繰り返される。

【0088】ステップS12において、ACK信号を受信したと判断された場合（すなわち、ICカード1が、リーダライタ2に装着された場合）、ステップS13において、制御部101は、ユーザが入力部106を用いて入力した操作を示す信号に従って、または、予め決められたサービスに基づいて、ユーザが希望するサービスに対応するサービスIDを、通信部91を介して、ICカード1に送信する。

【0089】ステップS14において、制御部101は、ICカード1から送信される信号（後述する図17のステップS25もしくはステップS26において、ICカード1が送信した信号）を受信する。ステップS15において、制御部101は、ステップS14において受信したデータは、ACK信号か否かを判断する。ステップS15において、受信した信号がACK信号ではない（すなわちNACK信号である）と判断された場合、ステップS16において、制御部101は、エラーメッセージに対応するデータを表示部105に出力して表示させ、処理を終了する（すなわち、処理は、図15のステップS3には進まない）。ステップS15において、受信した信号がACK信号であると判断された場合、処理は、図15のステップS3に進む。

【0090】次に、図17のフローチャートを参照して、図15のステップS2において、図16を用いて説明したリーダライタ2のサービス識別処理と並行して実行される、ICカード1のサービス識別処理について説明する。なお、ここでは、図3を用いて説明したICカ

10

20

30

40

50

ード1において処理が行われるものとして説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0091】ICカード1の制御部31は、ステップS21において、図16のステップS11において、リーダライタ2が送信したICカード検出コマンドを、通信部21を介して受信し、ステップS22において、リーダライタ2にACK信号を送信する。

【0092】制御部31は、ステップS23において、図16のステップS13において、リーダライタ2が送信したサービスIDを、通信部21を介して受信し、ステップS24において、受信したサービスIDは、ICカード1の対応するモジュール（ここでは、図3を用いて説明したICカード1における処理について説明しているので、ICカード処理部22のメモリ32に対応するが、例えば、図4を用いて説明したICカード1の場合、リーダライタ2が対応している方式により、共通鍵サービス処理部52のメモリ62あるいは、公開鍵サービス処理部のメモリ62に対応する）内に登録されているIDであるか否か、すなわち、ステップS23において受信したサービスIDが、図6を用いて説明したSRA46に登録されているか否かを判断する。

【0093】ステップS24において、受信したサービスIDが、モジュール内に登録されていると判断された場合、ステップS25において、制御部31は、通信部21を介して、リーダライタ2にACK信号を送信し、処理は、図15のステップS4に進む。ステップS24において、受信したサービスIDが、モジュール内に登録されていないと判断された場合、ステップS26において、制御部31は、通信部21を介して、リーダライタ2にNACK信号を送信し、処理が終了される（すなわち、図15のステップS4には進まない）。

【0094】次に、図18のフローチャートを参照して、複数のサービスに対応しているICカード1と、複数のサービスに対応しているリーダライタ2において、該当するICカード1とリーダライタ2が実行可能なサービスを抽出して、リーダライタ2の表示部105に表示させ、それらのサービスの中から、ユーザが所望するサービスを選択させることにより、サービス識別を行う場合における、図15のステップS1において実行される、リーダライタ2のサービス識別処理について説明する。

【0095】リーダライタ2の制御部101は、ステップS31において、サービスIDリスト送信コマンドを、ICカード1に、通信部91を介して送信し、ステップS32において、後述する図19のステップS52において、ICカード1が送信した、サービスIDリストを受信したか否かを判断する。ステップS32において、サービスIDリストを受信していないと判断された

場合、サービスIDリストを受信したと判断されるまで、ステップS32の処理が繰り返される。

【0096】ステップS32において、サービスIDリストを受信したと判断された場合、ステップS33において、制御部101は、受信したサービスIDリストに記載されているサービスIDは、リーダライタ2が対応しているサービスが含まれているか否か（すなわち、リーダライタ2のメモリ103に記憶されているサービスIDを含んでいるか否か）を判断する。

【0097】ステップS33において、受信したサービスIDリストに、リーダライタ対応サービスが含まれていると判断された場合、ステップS34において、制御部101は、サービスIDリストに含まれていた対応サービスが複数であるか否かを判断する。ステップS34において、対応サービスが複数ではない（すなわち1つだけである）と判断された場合、処理は、ステップS37に進む。

【0098】ステップS34において、対応サービスが複数であると判断された場合、制御部101は、ステップS35において、複数の対応サービスを表示部105に表示させるためのデータを生成し、表示部105に出力して表示させ、ステップS36において、入力部106から、ユーザが希望するサービスの入力を受ける。あるいは、サービスそれぞれに、優先度情報を含ませておき、複数の対応サービスのうちから、優先度の最も高いサービスが自動的に選択されるようにしてもよい。

【0099】ステップS37において、制御部101は、ステップS34において、対応サービスがただ1つであると判断された場合は、そのサービスに対応するサービスIDを、ステップS34において、対応サービスが複数であると判断された場合は、ステップS36において、ユーザが入力部106を用いて入力した希望するサービスに対応するサービスIDを、通信部91を介して、ICカード1に送信し、処理は、図15のステップS3に進む。

【0100】ステップS33において、受信したサービスIDリストに、リーダライタ対応サービスが含まれていないと判断された場合、制御部101は、ステップS38において、通信部91を介して、ICカード1にNACK信号を送信し、ステップS39において、図16のステップS16と同様の処理がなされ、処理が終了される（すなわち、処理は、図15のステップS3には進まない）。

【0101】次に、図19のフローチャートを参照して、図15のステップS2において、図18を用いて説明したリーダライタ2のサービス識別処理と並行して実行される、ICカード1のサービス識別処理について説明する。なお、ここでは、図3を用いて説明したICカード1において処理が行われるものとして説明するが、図4を用いて説明したICカード1によって処理が実行

される場合においても、基本的に同様の処理が実行される。

【0102】ICカード1の制御部31は、ステップS51において、リーダライタ2が、図18のステップS31において送信したサービスID送信コマンドを、通信部21を介して受信し、ステップS52において、自分自身が対応しているサービスIDリスト（すなわち、メモリ32のSRA46に登録されているサービスIDのリスト）を生成して、通信部21を介して、リーダライタ2に送信する。

【0103】制御部31は、ステップS53において、リーダライタ2が、図18のステップS37もしくはステップS38において、ICカード1に送信したデータを、通信部21を介して受信し、ステップS54において、リーダライタ2から受信したデータはNACK信号か否かを判断する。ステップS54において、受信した信号がNACK信号であると判断された場合（すなわち、受信したデータが、図18のステップS38において、リーダライタ2がICカード1に送信した信号である場合）、処理が終了される（すなわち、処理は、図15のステップS4には進まない）。

【0104】ステップS54において、リーダライタ2から受信したデータはNACK信号ではないと判断された場合（すなわち、受信したデータが、図18のステップS37において、リーダライタ2がICカード1に送信したサービスIDである場合）、ステップS55において、制御部31は、リーダライタ2から受信したサービスIDは、自分自身のメモリ32のSRA46に登録されているか否かを判断する。

【0105】ステップS55において、サービスIDが登録されていないと判断された場合、処理が終了される（すなわち、処理は、図15のステップS4には進まない）。ステップS55において、サービスIDが登録されていると判断された場合、処理は、図15のステップS4に進む。

【0106】次に、図20のフローチャートを参照して、図7（A）を用いて説明した認証用鍵情報を用いて認証鍵識別が行われる場合、図15のステップS3において実行される、リーダライタ2の認証鍵識別処理について説明する。

【0107】リーダライタ2の制御部101は、ステップS61において、図15のステップS1およびステップS2のサービス識別処理により識別されたサービスに対応するサービスID（ここでは、対応するサービスIDを、ID_Sとする）に属する認証鍵のうちの1つに対応する認証鍵IDを、メモリ103から読み出し、通信部91を介して、ICカード1に送信し、ステップS62において、後述する図21のステップS73もしくはステップS75において、ICカード1が送信するデータを受信する。

【0108】ステップS63において、制御部101は、ステップS62において、ICカード1から受信したデータは、ACK信号か否かを判断する。ステップS63において、ACK信号が受信されたと判断された場合、ステップS64において、制御部101は、暗号処理部33を制御して、ステップS61において、暗号処理部102の公開鍵処理部111もしくは共通鍵処理部112のうち、ICカード1に送信した認証鍵IDに対応する認証鍵を用いて認証処理を行う処理部を選択して制御することにより、ICカード1との相互認証処理および鍵共有処理を開始し、ICカード1とセッション鍵Ksesを共有し、相互認証処理が終了した後、処理が終了される。

【0109】ステップS63において、ACK信号が受信されていないと判断された場合（すなわち、NACK信号を受信したと判断された場合）、ステップS65において、図16のステップS16と同様の処理がなされ、処理が終了される。

【0110】次に、図21のフローチャートを参照して、図15のステップS4において、図20のリーダライタ2の認証鍵識別処理と並行して実行される、ICカード1の認証鍵識別処理について説明する。なお、ここでも、図3を用いて説明したICカード1により、処理が実行される場合について説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0111】ICカード1の制御部31は、ステップS71において、図20のステップS61において、リーダライタ2が送信した認証鍵IDを、通信部21を介して受信し、ステップS72において、ステップS71において受信した認証鍵IDは、メモリ32のSRA46のID_Sに関するデータが記憶されている領域に登録されているか否かを判断する。

【0112】ステップS72において、認証鍵IDが登録されていると判断された場合、制御部31は、ステップS73において、通信部21を介して、リーダライタ2にACK信号を送信し、ステップS74において、暗号処理部33の公開鍵処理部41もしくは共通鍵処理部42のうち、リーダライタ2に指定された認証鍵による認証処理を行う方を選択して制御することにより、相互認証処理を実行し、リーダライタ2とセッション鍵Ksesを共有し、相互認証処理の終了後、処理が終了される。ステップS72において、認証鍵IDが登録されていないと判断された場合、ステップS75において、制御部31は、通信部21を介して、リーダライタ2にNACK信号を送信し、処理が終了される。

【0113】図20および図21を用いて説明した処理においては、ICカード1とリーダライタ2は、図15のステップS1およびステップS2の処理により識別されたサービスのサービスIDに対応する、リーダライタ

2が指定した認証鍵により、相互認証を実行する。

【0114】例えば、あるサービスに対して共通鍵および公開鍵の2種類の認証鍵が用意されている場合、共通鍵に基づく認証処理により高速な処理を行うことをデフォルトとし、共通鍵のバージョンが古い場合には、公開鍵に基づいて認証処理を実施するようにしてもよい。

【0115】次に、図22のフローチャートを参照して、図15のステップS3において実行される、図15のステップS1およびステップS2の処理により識別されたサービスのサービスIDに対応するサービスに対して、共通鍵および公開鍵の2種類の認証鍵が用意されている場合のリーダライタ2の認証鍵識別処理について説明する。

【0116】リーダライタ2の制御部101は、ステップS81において、図15のステップS1およびステップS2の処理により識別されたサービスのサービスIDに対応する認証鍵の、共通鍵バージョン情報要求コマンドを、通信部91を介してICカード1に送信し、ステップS82において、後述する図23のステップS92において、ICカード1が送信した共通鍵バージョン情報を、通信部91を介して受信する。

【0117】ステップS83において、制御部101は、ステップS82において受信した共通鍵バージョン情報を基に、共通鍵バージョンが有効か否かを判断する。ステップS83において、共通鍵バージョンが有効であると判断された場合、ステップS84において、制御部101は、ICカード1に、共通鍵による相互認証開始コマンドを送信し、暗号処理部102の共通鍵処理部112を制御して、共通鍵による相互認証を開始し、ICカード1とセッション鍵Ksesを共有し、相互認証が終了した後、処理が終了される。

【0118】ステップS83において、共通鍵バージョンが有効ではないと判断された場合、ステップS85において、制御部101は、ICカード1に、公開鍵による相互認証開始コマンドを送信し、暗号処理部102の公開鍵処理部111を制御して、公開鍵による相互認証を開始し、ICカード1とセッション鍵Ksesを共有し、相互認証が終了した後、処理が終了される。

【0119】次に、図23のフローチャートを参照して、図15のステップS4において、図22を用いて説明したリーダライタ2の認証鍵識別処理と並行して実行される、ICカード1の認証鍵識別処理について説明する。なお、ここでも、図3を用いて説明したICカード1により、処理が実行される場合について説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0120】ICカード1の制御部31は、ステップS91において、図22のステップS81において、リーダライタ2が送信した共通鍵バージョン情報要求コマ

ンドを受信し、ステップS92において、共通鍵バージョン情報を、通信部21を介して、リーダライタ2に送信する。

【0121】制御部31は、ステップS93において、図22のステップS84もしくはステップS85において、リーダライタ2が送信した相互認証開始コマンドを受信し、ステップS94において、ステップS93において受信された相互認証開始コマンドは、共通鍵による相互認証開始コマンドであるか否かを判断する。

【0122】ステップS94において、共通鍵による相互認証開始コマンドであると判断された場合、ステップS95において、制御部31は、暗号処理部33の共通鍵処理部42を制御して、共通鍵による相互認証を開始し、リーダライタ2とセッション鍵Ksesを共有し、相互認証が終了した後、処理が終了される。

【0123】ステップS94において、共通鍵による相互認証開始コマンドではない（すなわち、公開鍵による相互認証開始コマンドである）と判断された場合、ステップS96において、制御部31は、暗号処理部33の公開鍵処理部41を制御して、公開鍵による相互認証を開始し、リーダライタ2とセッション鍵Ksesを共有し、相互認証が終了した後、処理が終了される。

【0124】図22および図23を用いて説明した処理により、ICカード1とリーダライタ2は、まず、認証速度の速い共通鍵による相互認証を実行しようとし、共通鍵による相互認証が行えない場合（例えば、対応する共通鍵のバージョンが古い場合など）、公開鍵を用いて、相互認証を実行する。

【0125】図22のステップS85および図23のステップS96の処理においては、公開鍵による相互認証が行われる。リーダライタ2のメモリ103のSRA46には、図24（A）に示されるリーダライタ2の証明書が記憶されている。また、ICカード1のメモリ32のSRA46には、図24（B）に示されるICカード1の証明書が記憶されている。

【0126】図24（A）および図24（B）に示されるように、それぞれの証明書には、証明書のバージョン番号、認証局が割り付ける証明書の通し番号、署名に用いたアルゴリズムとパラメータ、認証局の名前、証明書の有効期限、リーダライタ2、あるいはICカード1の名前（ID）、リーダライタ2の公開鍵Kpsp、あるいはICカード1の公開鍵Kpu、およびメッセージ全体に、図5を用いて説明したような不可逆的なハッシュ関数（データ圧縮関数）を作用させることで、メッセージダイジェストを作成し、メッセージダイジェストを、認証局の秘密鍵Kscalにより暗号化することによって作成された、デジタル署名から構成される。

【0127】次に、図25のフローチャートを参照して、署名生成処理について説明する。ここでは、楕円曲線暗号方式（楕円DSA署名）を用いて、デジタル署名

10

20

30

40

50

を生成する場合について説明する。ここでは、ICカード1の制御部31が、公開鍵処理部41のDSA署名生成・検証部72を制御することにより実行される処理について説明するが、リーダライタ2においても、同様の処理が実行されるので、リーダライタ2の処理についての説明は省略する。

【0128】ステップS101において、制御部31は、署名生成処理に必要なパラメータを認識する。すなわち、 p を標数、 a および b を楕円曲線の係数、楕円曲線を $y^2 = x^3 + ax + b$ 、 G を楕円曲線上のベースポイント、 r を G の位数、 M をメッセージ、 Ks を秘密鍵、 G および KsG を公開鍵とする。

【0129】公開鍵処理部41のDSA署名生成・検証部72は、ステップS102において、図示しない乱数生成部で、 $0 < u < r$ となる u を生成し、ステップS103において、ステップS102において生成された乱数 u を用いて、公開鍵 G を u 倍し、 $V = uG = (Xv, Yv)$ となる V を算出する。

【0130】DSA署名生成・検証部72は、ステップS104において、 $c = Xv \bmod r$ を算出し、ステップS105において、S104の計算結果に基づいて、 $c = 0$ であるか否かを判断する。ステップS105において、 $c = 0$ であると判断された場合、処理は、ステップS102に戻り、それ以降の処理が繰り返される。

【0131】ステップS105において、 $c = 0$ ではないと判断された場合、DSA署名生成・検証部72は、ステップS106において、メッセージ M のハッシュ値である $f = \text{SHA-1}(M)$ （ここでは、ハッシュ関数として、SHA-1が用いられる）を算出し、ステップS107において、 $d = [(f + cKs) / u] \bmod r$ を計算する。

【0132】ステップS108において、DSA署名生成・検証部72は、ステップS107の計算結果に基づいて、 $d = 0$ か否かを判断する。ステップS108において、 $d = 0$ であると判断された場合、処理は、ステップS102に戻り、それ以降の処理が繰り返される。ステップS108において、 $d = 0$ ではないと判断された場合、ステップS109において、DSA署名生成・検証部72は、署名データを (c, d) とし、処理が終了される。

【0133】このようにしてICカード1において生成されたデジタル署名を受信したリーダライタ2は、受信したデジタル署名を検証する処理を実施する。図26のフローチャートを参照して、署名検証処理について説明する。ここでは、リーダライタ2の制御部101が、公開鍵処理部41のDSA署名生成・検証部72を制御することにより実行される処理について説明するが、ICカード1においても、同様の処理が実行されるので、ICカード1の処理についての説明は省略する。

【0134】ステップS111において、制御部101

は、署名生成処理に必要なパラメータを認識する。すなわち、 p を標数、 a および b を楕円曲線の係数、楕円曲線を $y^2 = x^3 + ax + b$ 、 G を楕円曲線上のベースポイント、 r を G の位数、 M をメッセージ、 Ks を秘密鍵、 G および KsG を公開鍵とする。

【0135】公開鍵処理部41のDSA署名生成・検証部72は、ステップS112において、受信した署名データの c および d の値に基づいて、 $0 < c < r$ かつ $0 < d < r$ であるか否かを判断する。

【0136】ステップS112において、 $0 < c < r$ かつ $0 < d < r$ ではないと判断された場合、処理はステップS120に進む。ステップS112において、 $0 < c < r$ かつ $0 < d < r$ であると判断された場合、ステップS113において、DSA署名生成・検証部72は、メッセージ M のハッシュ値である $f = \text{SHA-1}(M)$ を算出し、ステップS114において、 $h = 1/d \bmod r$ を計算する。

【0137】DSA署名生成・検証部72は、ステップS114において算出された h の値を用いて、ステップS115において、 $h1 = fh$ 、 $h2 = ch \bmod r$ を算出し、ステップS116において、 $P = (Xp, Yp) = h1G + h2KsG$ を算出する。

【0138】ステップS117において、DSA署名生成・検証部72は、ステップS116の算出結果から、 P の値が無限遠点であるか否かを判断する。ここでは、 P の値が無限遠点である場合、ステップS116において、 $h1G + h2KsG$ の解を得ることができないことに基いて、 P の値が無限遠点であるか否かを判断することが可能である。ステップS117において、 P が無限遠点であると判断された場合、処理は、ステップS120に進む。

【0139】ステップS117において、 P の値が無限遠点ではないと判断された場合、ステップS118において、DSA署名生成・検証部72は、 $c = Xp \bmod r$ が成り立つか否かを判断する。ステップS118において、 $c = Xp \bmod r$ が成り立たないと判断された場合、処理は、ステップS120に進む。

【0140】ステップS118において、 $c = Xp \bmod r$ が成り立つと判断された場合、ステップS119において、DSA署名生成・検証部72は、受信した署名は正しいと判断し、処理が終了される。

【0141】ステップS112において、 $0 < c < r$ かつ $0 < d < r$ ではないと判断された場合、ステップS117において、 p が無限遠点であると判断された場合、もしくは、ステップS118において、 $c = Xp \bmod r$ が成り立たないと判断された場合、ステップS120において、DSA署名生成・検証部72は、受信した署名は正しくないと判断し、処理が終了される。

【0142】また、図7(B)を用いて説明した認証用鍵情報を用いて認証鍵識別が行われ、あるサービスに対

してレベル分けされた複数の認証鍵が格納されているような場合、低レベルの鍵から優先的に認証処理を開始し、その鍵のバージョンを判定し、その鍵のバージョンが古いとき、より高いレベルの認証鍵を用いて認証処理を行うようにしてもよい。

【0143】次に、図27のフローチャートを参照して、図15のステップS3において実行される、あるサービスに対してレベル分けされた複数の認証鍵が格納されている場合のリーダライタ2の認証鍵識別処理について説明する。

【0144】リーダライタ2の制御部101は、ステップS131において、通信部91を介して、鍵レベル交渉コマンドを、ICカード1に送信し、ステップS132において、後述する図28のステップS143において、ICカード1が送信する、レベルNにおける鍵バージョン情報Vを、通信部91を介して受信する。

【0145】ステップS133において、制御部101は、ステップS132において受信した鍵バージョン情報VのレベルNは、 $N > 0$ であるか否かを判断する。ステップS133において、 $N > 0$ ではないと判断された

場合、処理はステップS137に進む。

【0146】ステップS133において、 $N > 0$ であると判断された場合、ステップS134において、制御部101は、ステップS132において受信した鍵バージョン情報Vに基づいて、レベルNにおける鍵バージョン情報は有効か否かを判断する。

【0147】ステップS134において、レベルNにおける鍵バージョンが有効ではないと判断された場合（すなわち、鍵のバージョンが古いと判断された場合）、ステップS135において、制御部101は、通信部91を介して、ICカード1にNACK信号を送信し、処理はステップS132に戻り、それ以降の処理が繰り返される。

【0148】ステップS134において、レベルNにおける鍵バージョンは有効であると判断された場合、ステップS136において、制御部101は、通信部91を介して、ICカード1にACK信号を送信し、処理が終了される。

【0149】ステップS133において、 $N > 0$ ではないと判断された場合、ステップS137において、図16のステップS16と同様の処理がなされ、処理が終了される。

【0150】次に、図28のフローチャートを参照して、図27を用いて説明したリーダライタ2の認証鍵識別処理と並行して実行される、ICカード1の認証鍵識別処理について説明する。なお、ここでも、図3を用いて説明したICカード1により、処理が実行される場合について説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0151】ICカード1の制御部31は、ステップS141において、図27のステップS131において、リーダライタ2が送信した鍵レベル交渉コマンドを受信し、ステップS142において、現在の鍵レベルNを、 $N = 1$ にセットする。

【0152】制御部31は、ステップS143において、現在の鍵レベルNと、そのレベルにおける鍵バージョン情報Vを、通信部21を介して、リーダライタ2に送信し、ステップS144において、図27のステップS135もしくはステップS136において、リーダライタ2が送信したデータを受信する。

【0153】ステップS145において、制御部31は、ステップS144において、リーダライタ2から受信した信号は、ACK信号であるか否かを判断する。ステップS145において、リーダライタ2から受信した信号はACK信号ではないと判断された場合、制御部31は、ステップS146において、 $N = N + 1$ とし、ステップS147において、Nの値が所定の最大レベルを超えているか否かを判断する。

【0154】ステップS147において、Nが最大レベルを超えていないと判断された場合、処理はステップS143に戻り、それ以降の処理が繰り返される。ステップS147において、Nが最大レベルを超えていると判断された場合、ステップS148において、制御部31は、現在のレベルを $N = 0$ （ $N = 0$ は、例外状態を示すものとする）とし、処理はステップS143に戻り、それ以降の処理が繰り返される。

【0155】ステップS145において、リーダライタ2から受信した信号はACK信号であると判断された場合、処理が終了される。

【0156】図15乃至図28を用いて、ICカード1と、リーダライタ2のサービス識別および認証鍵識別に関する処理について説明したが、例えば、図2を用いて説明したサービス登録用リーダライタ2-11に、ICカード1を装着し、新たなサービスの登録を実行する場合、およびサービスの削除を実行する場合には、図10を用いて説明したように、サービス登録用リーダライタ2-11のメモリ103に記憶されているサービス登録用の認証鍵Kregを用いて認証処理を行うため、図15乃至図28を用いて説明したような相互認証処理を用いなくてもよい。

【0157】次に、図29のフローチャートを参照して、サービス登録用リーダライタ2-11のサービス登録処理について説明する。

【0158】サービス登録用リーダライタ2-11の制御部101は、ステップS151において、通信部91を介して、サービス登録コマンドを、ICカード1に送信し、ステップS152において、ICカード1と、サービス登録用鍵Kregによる相互認証を行い、セッション鍵Ksesを共有する。

【0159】制御部101は、ステップS153において、空き領域確認コマンドを、通信部91を介してICカード1に送信し、ステップS154において、後述する図30のステップS175もしくはステップS176においてICカード1から送信されるデータを受信する。

【0160】ステップS155において、制御部101は、ステップS154において、ICカード1から受信した信号はACK信号であるか否かを判断する。ステップS155において、ICカード1から受信した信号がACK信号であると判断された場合、制御部101は、ステップS156において、暗号処理部102の共通鍵処理部112を制御して、ICカード1のメモリ32に新たに登録する登録データを、セッション鍵Ksesで暗号化させ、ステップS157において、暗号化データを、通信部91を介して、ICカード1に送信する。

【0161】制御部101は、ステップS158において、後述する図30のステップS180において、ICカード1が送信したデータ登録完了通知を、通信部91を介して受信し、ステップS159において、サービス認証によるサービス削除許可フラグを送信し、処理が終了される。

【0162】ステップS155において、ICカード1から受信した信号がACK信号ではないと判断された場合、ステップS160において、図16のステップS16と同様の処理がなされ、処理が終了される。

【0163】次に、図30のフローチャートを参照して、図29を用いて説明した、サービス登録用リーダライタ2-11のサービス登録処理と並行して実行される、ICカード1のサービス登録処理について説明する。なお、ここでも、図3を用いて説明したICカード1により、処理が実行される場合について説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0164】ステップS171において、ICカード1の制御部31は、通信部21を介して、図29のステップS151において、サービス登録用リーダライタ2-11が送信したサービス登録コマンドを受信する。

【0165】制御部31は、ステップS172において、ICカード1と、サービス登録用鍵Kregによる相互認証を行い、セッション鍵Ksesを共有し、ステップS173において、通信部21を介して、図29のステップS153において、サービス登録用リーダライタ2-11が送信した、空き領域確認コマンドを受信する。

【0166】ステップS174において、制御部31は、メモリ32のSRA46に、登録データ用の空き領域があるか否かを判断する。ステップS174において、空き領域がないと判断された場合、ステップS175において、制御部31は、サービス登録用リーダライ

タ2-11に、通信部21を介して、NACK信号を送信し、処理が終了される。

【0167】ステップS174において、空き領域があると判断された場合、ステップS176において、制御部31は、サービス登録用リーダライタ2-11に、通信部21を介して、ACK信号を送信する。

【0168】制御部31は、ステップS177において、図29のステップS157において、サービス登録用リーダライタ2-11が送信した暗号化データを、通信部21を介して受信し、ステップS178において、暗号処理部33の共通鍵処理部42を制御して、ステップS177において受信した暗号化データを、セッション鍵Ksesを用いて復号させる。

【0169】ステップS179において、制御部31は、ステップS178において、セッション鍵Ksesにより復号されたデータを、メモリ32に供給し、SRA46のService Individual Info領域およびSRT45に登録させる。

【0170】制御部31は、ステップS180において、データの登録完了を、通信部21を介して、サービス登録用リーダライタ2-11に通知し、ステップS181において、図29のステップS159において、サービス登録用リーダライタ2-11が送信した、サービス認証によるサービス削除許可フラグを受信し、サービス削除許可フラグを、メモリ32のSRA46のService Individual Info領域に設定し、処理が終了される。

【0171】次に、図31のフローチャートを参照して、サービス登録用リーダライタ2-11のサービス削除処理について説明する。

【0172】ステップS191において、サービス登録用リーダライタ2-11の制御部101は、ユーザが、入力部106を用いて入力した、削除するサービスに対応するサービスIDの入力を受ける（ここでは、対応するサービスIDが、ID_Sであるサービスが削除されるものとする）。

【0173】ステップS192において、図29のステップS152と同様の処理がなされる。制御部101は、ステップS193において、通信部91を介して、ICカード1に、ID_S領域削除コマンドを送信し、ステップS194において、後述する図32のステップS205においてICカード1が送信した、エラーメッセージを受信したか否かを判断する。

【0174】ステップS194において、エラーメッセージを受信したと判断された場合、ステップS195において、図16のステップS16と同様の処理がなされ、処理が終了される。ステップS194において、エラーメッセージを受信しなかったと判断された場合、処理が終了される。

【0175】次に、図32のフローチャートを参照して、図31を用いて説明した、サービス登録用リーダ

10

20

30

40

50

イタ2-11のサービス削除処理と並行して実行される。ICカード1のサービス削除処理について説明する。なお、ここでも、図3を用いて説明したICカード1により、処理が実行される場合について説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0176】ステップS201において、図30のステップS172と同様の処理が実行される。ICカード1の制御部31は、ステップS202において、図31のステップS193において、サービス登録用リーダライタ2-11が送信した、ID_S領域削除コマンドを受信し、ステップS203において、ID_S領域に対応するデータがあるか否かを確認することなどにより、ステップS202において受信したID_S領域削除コマンドの正当性が検証されたか否かを判断する。

【0177】ステップS203において、ID_S領域削除コマンドの正当性が検証されたと判断された場合、ステップS204において、制御部31は、メモリ32のSRT45およびSRA46から、ID_Sに対応する領域を削除し、処理が終了される。

【0178】ステップS203において、ID_S領域削除コマンドの正当性が検証されなかったと判断された場合、ステップS205において、制御部31は、通信部21を介して、サービス登録用リーダライタ2-11に、エラーメッセージを送信し、処理が終了される。

【0179】図31および図32を用いて説明したサービス削除処理は、一般リーダライタ2-12とICカード1とで実行することも可能である。図33のフローチャートを参照して、一般リーダライタ2-12のサービス削除処理について説明する。

【0180】ステップS211において、図16、もしくは図18を用いて説明した、リーダライタ2のサービス識別処理が実行され、ステップS212において、図20、図22、もしくは図27を用いて説明したリーダライタ2の認証鍵識別処理が実行され、ステップS213において、図31のステップS193と同様の処理が実行される。

【0181】ステップS214において、一般リーダライタ2-12の制御部101は、後述する図34のステップS227もしくはステップS228において、ICカード1が送信する信号を受信する。そして、ステップS215およびステップS216において、図16のステップS15およびステップS16と同様の処理が実行され、処理が終了される。

【0182】次に、図34のフローチャートを参照して、図33を用いて説明した、一般リーダライタ2-12のサービス削除処理と並行して実行される、ICカード1のサービス削除処理について説明する。なお、ここでも、図3を用いて説明したICカード1により、処理

が実行される場合について説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0183】ステップS221において、図17、もしくは図19を用いて説明した、ICカード1のサービス識別処理が実行され、ステップS232において、図21、図23、もしくは図28を用いて説明したICカード1の認証鍵識別処理が実行される。

【0184】ステップS223において、制御部31は、図33のステップS213において、一般リーダライタ2-12が送信した、ID_S領域削除コマンドを、通信部21を介して受信する。ステップS224において、図32のステップS203と同様の処理が実行される。

【0185】ステップS224において、コマンドの正当性が検証されなかったと判断された場合、処理は、ステップS228に進む。ステップS224において、コマンドの正当性が検証されたと判断された場合、ステップS225において、制御部31は、メモリ32のSRA46のService Individual Info領域に、サービス削除許可フラグが設定されているか否かを判断する。

【0186】ステップS225において、サービス削除許可フラグが設定されていないと判断された場合、処理は、ステップS228に進む。ステップS225において、サービス削除許可フラグが設定されていると判断された場合、ステップS226において、図32のステップS204と同様の処理がなされ、ステップS227において、制御部31は、通信部21を介して、一般リーダライタ2-12にACK信号を送信し、処理が終了される。

【0187】ステップS224において、コマンドの正当性が検証されなかったと判断された場合、もしくは、ステップS225において、サービス削除許可フラグが設定されていないと判断された場合、ステップS228において、制御部31は、通信部21を介して、一般リーダライタ2-12にNACK信号を送信し、処理が終了される。

【0188】次に、図35のフローチャートを参照して、ユーザが、一般リーダライタ2-12で、ICカード1に登録されているサービスを受ける場合に実行される、一般リーダライタ2-12のサービス取得処理について説明する。

【0189】ステップS231において、図16、もしくは図18を用いて説明した、リーダライタ2のサービス識別処理が実行され、ステップS232において、図20、図22、もしくは図27を用いて説明したリーダライタ2の認証鍵識別処理が実行される。

【0190】ステップS233において、一般リーダライタ2-12の制御部101は、通信部91を介して、ICカード1に、ID_S領域のデータ要求コマンドを

送信する。

【0191】制御部101は、ステップS234において、後述する図36のステップS245において、ICカード1から送信されるデータを受信し、ステップS235において、暗号処理部102の共通鍵処理部112を制御して、ステップS234において受信した暗号化データを、セッション鍵Ksesを用いて復号させる。制御部101は、復号されたデータを用いて、例えば、電子マネーの減算や加算などの所定のデータ処理を行い、処理が終了される。

【0192】次に、図36のフローチャートを参照して、図35を用いて説明した、一般リーダライタ2-12のサービスデータ取得処理と並行して実行される、ICカード1のサービスデータ取得処理について説明する。なお、ここでも、図3を用いて説明したICカード1により、処理が実行される場合について説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0193】ステップS241において、図17、もしくは図19を用いて説明した、ICカード1のサービス識別処理が実行され、ステップS232において、図21、図23、もしくは図28を用いて説明したICカード1の認証鍵識別処理が実行される。

【0194】ステップS243において、ICカード1の制御部31は、通信部21を介して、図35のステップS233において、一般リーダライタ2-12が送信した、ID_S領域のデータ要求コマンドを受信する。制御部31は、ステップS244において、暗号処理部33の共通鍵処理部42を制御して、メモリ32のID_Sに対応する領域に登録しているデータを、セッション鍵Ksesを用いて暗号化させ、ステップS245において、通信部21を介して、暗号化したデータを一般リーダライタ2-12に送信し、処理が終了される。

【0195】また、ICカード1と一般リーダライタ2-12において、あるサービスに関する情報の授受がなされている場合においても、図8を用いて説明したSRT45に、対応するパーミッション情報が記録されている場合、現在情報の授受が行われている以外のサービスに関する情報の授受を行うことが可能である。図37のフローチャートを参照して、ID_S以外のサービスIDに対応するサービスの実行中に行われる、一般リーダライタ2-12のサービスデータ取得処理について説明する。

【0196】ステップS251乃至ステップS254において、図35のステップS231乃至ステップS234と同様の処理が実行される。ステップS255において、一般リーダライタ2-12の制御部101は、ステップS254において、ICカード1から受信したデータは、NACK信号か否かを判断する。

【0197】ステップS255において、受信したデータがNACK信号ではないと判断された場合、ステップS256において、図35のステップS235と同様の処理が実行され、処理が終了される。ステップS255において、受信したデータがNACK信号であると判断された場合、図16のステップS16と同様の処理がなされ、処理が終了される。

【0198】次に、図38のフローチャートを参照して、図37を用いて説明した、一般リーダライタ2-12のサービスデータ取得処理と並行して実行される、ICカード1のサービスデータ取得処理について説明する。なお、ここでも、図3を用いて説明したICカード1により、処理が実行される場合について説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0199】ステップS261乃至ステップS263において、図34のステップS241乃至ステップS243と同様の処理が実行される。なお、ステップS261では、サービスID_Sとは異なる、サービスID_Tの認証が行われるものとする。ステップS264において、ICカード1の制御部31は、メモリ32のSRT45およびSRA46に、ステップS263において受信したデータ要求コマンドに対応するID_S領域が登録されているか否かを判断する。ステップS264において、ID_S領域が登録されていないと判断された場合、処理は、ステップS269に進む。

【0200】ステップS264において、ID_S領域が登録されていると判断された場合、制御部31は、ステップS265において、メモリ32のSRT45の、ID_Sに対応するパーミッション情報フィールドから、ID_Sのパーミッション情報を取得し、ステップS266において、ID_T認証時に、ID_Sのデータの読み込みが許可されているか否かを判断する（すなわち、SRT45のID_Sに対応するパーミッション情報フィールドに、ID_Tによる認証時に、データの読み出し許可、すなわち、rもしくはrwが記載されているか否かを判断する）。ステップS266において、データの読み込みが許可されていないと判断された場合、処理はステップS269に進む。

【0201】ステップS266において、データの読み込みが許可されていると判断された場合、ステップS267およびステップS268において、図36のステップS244およびステップS245と同様の処理が実行され、処理が終了される。

【0202】ステップS264において、ID_S領域が登録されていないと判断された場合、もしくは、ステップS266において、データの読み込みが許可されていないと判断された場合、ステップS269において、制御部31は、通信部21を介して、一般リーダライタ

10

20

30

40

50

2-12にNACK信号を送信し、処理が終了される。

【0203】図35乃至図48を用いて説明したサービスデータ取得処理によって、ICカード1から一般リーダライタ2-12にデータが取得され、所定の処理がなされたあと、一般リーダライタ2-12は、必要に応じて、ICカード1のメモリ32のSRT45もしくはSRA46の所定の領域に対して、データを書き込む処理を実行する。

【0204】次に、図39のフローチャートを参照して、一般リーダライタ2-12のサービスデータ書き込み処理について説明する。

【0205】ステップS281において、図16、もしくは図18を用いて説明した、リーダライタ2のサービス識別処理が実行され、ステップS282において、図20、図22、もしくは図27を用いて説明したリーダライタ2の認証鍵識別処理が実行される。

【0206】一般リーダライタ2-12の制御部101は、ステップS283において、ICカード1のメモリ32に書き込むために、ICカード1に送信するデータを、暗号処理部102の共通鍵処理部112を制御して、セッション鍵Ksesを用いて暗号化させ、ステップS284において、ICカード1に、データ書き込みコマンドと、ステップS284において暗号化したデータを、通信部91を介して送信し、処理が終了される。

【0207】次に、図40のフローチャートを参照して、図39を用いて説明した、一般リーダライタ2-12のサービスデータ書き込み処理と並行して実行される、ICカード1のサービスデータ書き込み処理について説明する。なお、ここでも、図3を用いて説明したICカード1により、処理が実行される場合について説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0208】ステップS291において、図17、もしくは図19を用いて説明した、ICカード1のサービス識別処理が実行され、ステップS232において、図21、図23、もしくは図28を用いて説明したICカード1の認証鍵識別処理が実行される。

【0209】ステップS293において、制御部31は、通信部21を介して、図39のステップS284において、一般リーダライタ2-12が送信した、データ書き込みコマンドと暗号化データを受信する。制御部31は、ステップS294において、暗号処理部33の共通鍵処理部42を制御して、受信したデータを、セッション鍵Ksesを用いて復号させ、ステップS295において、復号したデータを、メモリ32のSRT45およびSRA46のID_Sに対応するサービス格納領域へ書き込み、処理が終了される。

【0210】また、ICカード1と一般リーダライタ2-12において、あるサービスに関する情報の授受がな

されている場合においても、図8を用いて説明したSRT45に、対応するパーミッション情報が記録されている場合、図37および図38を用いて説明したサービスデータ取得処理と同様に、現在情報の授受がなされている以外のサービスに関するサービスデータ書き込み処理を実行することが可能である。図41のフローチャートを参照して、ID_S以外のサービスIDに対応するサービスの実行中に行われる、一般リーダライタ2-12のサービスデータ書き込み処理について説明する。

【0211】ステップS301乃至ステップS304において、図39のステップS281乃至ステップS284と同様の処理が実行される。そして、ステップS305およびステップS306において、図16のステップS15およびステップS16と同様の処理がなされ、処理が終了される。

【0212】次に、図42のフローチャートを参照して、図41を用いて説明した、一般リーダライタ2-12のサービスデータ書き込み処理と並行して実行される、ICカード1のサービスデータ書き込み処理について説明する。なお、ここでも、図3を用いて説明したICカード1により、処理が実行される場合について説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0213】ステップS311乃至ステップS313において、図40のステップS291乃至ステップS293と同様の処理が実行される。なお、ステップS311では、サービスID_Sとは異なる、サービスID_Tの認証が行われるものとする。ステップS314およびステップS315において、図38のステップS264およびステップS265と同様の処理がなされ、ステップS314において、ID_S領域が登録されていないと判断された場合、処理は、ステップS320に進む。

【0214】ステップS316において、制御部31は、ID_T認証時に、ID_Sのサービスに対して、データの書き込みが許可されているか否かを判断する（すなわち、SRT45のID_Sに対応するパーミッション情報フィールドに、ID_T認証時のデータの書き込み許可、すなわち、rwが記載されているか否かを判断する）。ステップS316において、データの書き込みが許可されていないと判断された場合、処理はステップS320に進む。

【0215】ステップS316において、データの書き込みが許可されていると判断された場合、ステップS317およびステップS318において、図40のステップS294およびステップS295と同様の処理が実行される。ステップS319において、制御部31は、通信部21を介して、一般リーダライタ2-12にACK信号を送信し、処理が終了される。

【0216】ステップS314において、ID_S領域

が登録されていないと判断された場合、もしくは、ステップ S 316 において、データの書き込みが許可されていないと判断された場合、ステップ S 320 において、制御部 31 は、通信部 21 を介して、一般リーダライタ 2-12 に NACK 信号を送信し、処理が終了される。

【0217】以上説明したように、一般リーダライタ 2-12 に、IC カード 1 を装着し、各種サービスを受けるためには、サービス毎に定められた共通鍵、もしくは公開鍵を用いて認証処理を行わなければならない。これらの認証鍵は、セキュリティの維持のために、しばしばバージョンアップされる（すなわち、鍵が変更される）。ユーザは、図 2 を用いて説明したバージョンアップ用リーダライタ 2-14、もしくは一般リーダライタ 2-12 に、IC カード 1 を装着し、図 43 乃至図 47 を用いて後述する鍵バージョンアップ処理を実行させることにより、自分自身が管理している IC カード 1 に登録されている認証鍵を、できるだけ最新に近いバージョンの認証鍵にバージョンアップするようにしなければならない。

【0218】次に、図 43 を参照して、サービス毎に定められたバージョンアップ用鍵（図 6 および図 14 を用いて説明したバージョンアップ用鍵 K_{ake_vup} ）を用いて実行される、バージョンアップ用リーダライタ 2-14 の鍵バージョンアップ処理について説明する。

【0219】ステップ S 331 において、図 16、もしくは図 18 を用いて説明した、リーダライタ 2 のサービス識別処理が実行され、ステップ S 332 において、図 20、図 22、もしくは図 27 を用いて説明したリーダライタ 2 の認証鍵識別処理が実行される。

【0220】ステップ S 333 において、バージョンアップ用リーダライタ 2-14 の制御部 101 は、暗号処理部 102 の共通鍵処理部 112 を制御して、バージョンアップを行う認証鍵に対応する認証鍵 ID を、セッション鍵 K_{ses} を用いて暗号化させ、IC カード 1 に送信する。ステップ S 334 において、制御部 101 は、後述する図 44 のステップ S 355 もしくはステップ S 360 において、IC カード 1 が送信する信号を受信する。

【0221】ステップ S 335 において、制御部 101 は、ステップ S 334 において IC カード 1 から受信した信号は ACK 信号であるか否かを判断する。ステップ S 335 において、受信した信号が ACK 信号ではないと判断された場合、処理は、ステップ S 339 に進む。ステップ S 335 において、受信した信号が ACK 信号であると判断された場合、ステップ S 336 において、制御部 101 は、バージョンアップを行う認証鍵に対応する最新バージョン情報と、認証鍵 K_{ake} をメモリ 103 から読み出し、暗号処理部 102 の共通鍵処理部 112 を制御して、セッション鍵 K_{ses} を用いて暗号化させ、通信部 91 を介して、IC カード 1 に送信する。

【0222】そして、ステップ S 337 において、IC

カード 1 が、後述する 44 のステップ S 359 もしくはステップ S 360 において送信した信号を受信する。ステップ S 338 において、ステップ S 335 と同様の処理がなされ、ステップ S 338 において、受信した信号が ACK 信号であると判断された場合、処理が終了される。ステップ S 335 およびステップ S 338 において、受信した信号が ACK 信号ではないと判断された場合、ステップ S 339 において、図 16 のステップ S 16 と同様の処理がなされ、処理が終了される。

【0223】次に、図 44 のフローチャートを参照して、図 43 を用いて説明した、バージョンアップ用リーダライタ 2-14 の鍵バージョンアップ処理と並行して実行される、IC カード 1 の鍵バージョンアップ処理について説明する。なお、ここでも、図 3 を用いて説明した IC カード 1 により、処理が実行される場合について説明するが、図 4 を用いて説明した IC カード 1 によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0224】ステップ S 351 において、図 17、もしくは図 19 を用いて説明した、IC カード 1 のサービス識別処理が実行され、ステップ S 352 において、図 21、図 23、もしくは図 28 を用いて説明した IC カード 1 の認証鍵識別処理が実行される。

【0225】ステップ S 353 において、制御部 31 は、通信部 21 を介して、図 43 のステップ S 333 において、バージョンアップ用リーダライタ 2-14 が送信した、暗号化された認証鍵 ID を受信し、暗号処理部 33 の共通鍵処理部 42 を制御して、受信したデータを、セッション鍵 K_{ses} を用いて復号させる。ステップ S 354 において、制御部 31 は、復号したデータを基に、メモリ 32 の SRT 45 および SRA 46 の ID_S に、対応する認証鍵 ID が存在するか否かを判断する。ステップ S 354 において、認証鍵 ID が存在しないと判断された場合、処理は、ステップ S 360 に進む。

【0226】ステップ S 354 において、認証鍵 ID が存在すると判断された場合、制御部 31 は、ステップ S 355 において、通信部 21 を介して、バージョンアップ用リーダライタ 2-14 に、ACK 信号を送信し、ステップ S 356 において、図 43 のステップ S 336 において、バージョンアップ用リーダライタ 2-14 が送信した、暗号化された最新バージョン情報と認証鍵 K_{ake} を、通信部 21 を介して受信し、暗号処理部 33 の共通鍵処理部 42 を制御して、受信したバージョン情報を、セッション鍵 K_{ses} を用いて復号させる。

【0227】ステップ S 357 において、制御部 31 は、復号したデータを基に、受信したバージョン情報は正しいか否か（すなわち、自分自身がすでに保有している認証鍵のバージョン情報より新しいバージョンであるか否か）を判断する。ステップ S 357 において、バー

ジョン情報が正しくないと判断された場合、処理は、ステップS360に進む。

【0228】ステップS357において、バージョン情報は正しいと判断された場合、制御部31は、暗号処理部33の共通鍵処理部42を制御して、認証鍵Kakeを、セッション鍵Ksesを用いて復号させ、メモリ32のSRA46における、認証鍵Kakeが記載される領域に書き込み、ステップS359において、バージョンアップ用リーダーライタ2-14に、通信部21を介してACK信号を送信し、処理が終了される。

【0229】ステップS354において、認証鍵IDが存在しないと判断された場合、およびステップS357において、バージョン情報が正しくないと判断された場合、ステップS360において、制御部31は、バージョンアップ用リーダーライタ2-14に、通信部21を介してNACK信号を送信し、処理が終了される。

【0230】また、ICカード1と一般リーダーライタ2-12において、あるサービスに関する情報の授受がなされている場合において、図8を用いて説明したSRT45に、対応するパーミッション情報が記録されている場合、図37および図38を用いて説明したサービスデータ取得処理や、図41および図42を用いて説明したサービスデータ書き込み処理と同様に、現在情報の授受がなされている以外のサービスに関する鍵バージョンアップ処理を実行することが可能である。図45のフローチャートを参照して、ID_S以外のサービスIDに対応するサービスの実行中に行われる、一般リーダーライタ2-12の鍵バージョンアップ処理について説明する。

【0231】ステップS371およびステップS372において、図44のステップS331およびステップS332と同様の処理が実行される。そして、一般リーダーライタ2-12の制御部101は、ステップS373において、ID_Sに対応するサービスの認証鍵のバージョンアップコマンドを、通信部91を介してICカード1に送信し、ステップS374において、後述する図46のステップS397もしくは図47のステップS405において、ICカード1が送信するデータを受信し、ステップS375において、ICカード1から受信した信号は、ACK信号か否かを判断する。

【0232】ステップS375において、受信した信号がACK信号でないと判断された場合、処理は、ステップS382に進む。ステップS375において、受信した信号がACK信号であると判断された場合、ステップS376乃至ステップS382において、図43のステップS333乃至ステップS339と同様の処理がなされ、処理が終了される。

【0233】次に、図46および図47のフローチャートを参照して、図45を用いて説明した、バージョンアップ用リーダーライタ2-14の鍵バージョンアップ処理と並行して実行される、ICカード1の鍵バージョンア

ップ処理について説明する。なお、ここでも、図3を用いて説明したICカード1により、処理が実行される場合について説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0234】ステップS391およびステップS392において、図44のステップS351およびステップS352と同様の処理が実行される。なお、ステップS391では、サービスID_Sとは異なる、サービスID_Tの認証が行われるものとする。ステップS393において、制御部31は、図45のステップS373において、バージョンアップ用リーダーライタ2-14が送信した、ID_Sの認証鍵のバージョンアップコマンドを受信する。

【0235】ステップS394およびステップS395において、図38のステップS264およびステップS265と同様の処理がなされ、ステップS394において、ID_S領域が登録されていないと判断された場合、処理は、ステップS405に進む。

【0236】ステップS396において、制御部31は、ID_T認証時に、ID_Sの認証鍵のバージョンアップが許可されているか否かを判断する（すなわち、SRT45のID_Sに対応するパーミッション情報フィールドに、ID_T認証時のvupの許可が記載されているか否かを判断する）。ステップS396において、認証鍵のバージョンアップが許可されていないと判断された場合、処理は、ステップS405に進む。

【0237】ステップS396において、認証鍵のバージョンアップが許可されていると判断された場合、ステップS397において、制御部31は、通信部21を介して、バージョンアップ用リーダーライタ2-14に、ACK信号を送信する。

【0238】そして、ステップS398乃至ステップS405において、図44のステップS353乃至ステップS360と同様の処理が実行され、処理が終了される。

【0239】次に、図48乃至図51のフローチャートを参照して、図13を用いて説明したモジュール間通信について説明する。モジュール間通信は、図4を用いて説明したICカード1と、モジュール間通信用リーダーライタ2-13によって実行される。ここでは、図4を用いて説明したICカード1の通信部51および共通鍵サービス処理部52を、図13を用いて説明した共通鍵モジュール122とし、図4を用いて説明した通信部53および公開鍵サービス処理部54を、図13を用いて説明した公開鍵モジュール121として説明する。

【0240】まず、図48のフローチャートを参照して、共通鍵モジュール122が、モジュール間通信用リーダーライタ2-13と共有するセッション鍵と、公開鍵モジュール121が、モジュール間通信用リーダーライタ

10

20

30

40

50

2-13と共有するセッション鍵とが異なる場合におけるモジュール間通信について説明する。

【0241】ステップS411において、モジュール間通信用リーダライタ2-13は、図16、もしくは図18を用いて説明した、リーダライタ2のサービス識別処理を実行し、ステップS412において、ICカード1の公開鍵モジュール121は、図17、もしくは図19を用いて説明した、ICカード1のサービス識別処理を実行し、モジュール間リーダライタ2-13と、公開鍵モジュール121の間で、セッション鍵Kses1を共有する。

【0242】ステップS413において、モジュール間通信用リーダライタ2-13は、図16、もしくは図18を用いて説明した、リーダライタ2のサービス識別処理を実行し、ステップS414において、ICカード1の共通鍵モジュール122は、図17、もしくは図19を用いて説明した、ICカード1のサービス識別処理を実行し、モジュール間リーダライタ2-13と、共通鍵モジュール122の間で、セッション鍵Kses2を共有する。

【0243】ステップS415において、モジュール間通信用リーダライタ2-13の制御部101は、ステップS411およびステップS413において実行されたリーダライタ2のサービス識別処理において得られたICカード1のカードIDを基に、公開鍵モジュール121と、共通鍵モジュール122の2つのカードIDが一致したか否かを判断する。ステップS415において、カードIDが一致しないと判断された場合、ステップS416において、図16のステップS16と同様の処理が実行される。

【0244】ステップS415において、2つのカードIDが一致すると判断された場合、ステップS417において、モジュール間通信用リーダライタ2-13の制御部101は、モジュールデータ移動コマンドを公開鍵モジュール121に送信する。

【0245】公開鍵モジュール121の制御部61は、ステップS418において、モジュールデータ移動開始コマンドをモジュール間通信用リーダライタ2-13から受信し、暗号処理部33の、共通鍵処理部42を制御して、移動するデータをセッション鍵Kses1で暗号化させ、ステップS419で、暗号化データをモジュール間通信用リーダライタ2-13に送信する。

【0246】モジュール間通信用リーダライタ2-13の制御部101は、ステップS420において、暗号処理部102の、共通鍵処理部112を制御して、受信したデータをセッション鍵Kses1で復号し、ステップS421において、データをセッション鍵Kses2で暗号化させ、共通鍵モジュール122に送信する。共通鍵モジュール122の制御部61は、ステップS422において、暗号処理部63の、共通鍵処理部42を制御して、

受信したデータをセッション鍵Kses2で復号させ、ステップS423において、復号したデータをメモリ62の対応する領域に保存して利用する。

【0247】次に、図49のフローチャートを参照して、共通鍵モジュール122が、モジュール間通信用リーダライタ2-13と共有するセッション鍵と、公開鍵モジュール121が、モジュール間通信用リーダライタ2-13と共有するセッション鍵とが同一である場合におけるモジュール間通信について説明する。

【0248】ステップS431において、モジュール間通信用リーダライタ2-13は、図16、もしくは図18を用いて説明した、リーダライタ2のサービス識別処理を実行し、ステップS432において、ICカード1の公開鍵モジュール121は、図17、もしくは図19を用いて説明した、ICカード1のサービス識別処理を実行し、モジュール間リーダライタ2-13と、公開鍵モジュール121の間で、セッション鍵Kses1を共有する。

【0249】ステップS433において、モジュール間通信用リーダライタ2-13は、図16、もしくは図18を用いて説明した、リーダライタ2のサービス識別処理を実行し、ステップS434において、ICカード1の共通鍵モジュール122は、図17、もしくは図19を用いて説明した、ICカード1のサービス識別処理を実行し、モジュール間リーダライタ2-13と、共通鍵モジュール122の間で、セッション鍵Kses1を共有する。

【0250】ステップS435乃至ステップS439において、図48のステップS415乃至ステップS419と同様の処理が実行される。そして、ステップS440において、モジュール間通信用リーダライタ2-13の制御部101は、受信したデータを、共通鍵モジュール122に送信する。図48のステップS420およびステップS421においては、受信したデータをセッション鍵Kses1で復号し、復号したデータをセッション鍵Kses2で暗号化した後に共通鍵モジュール122に送信したが、ここでは、共通鍵モジュール122も、セッション鍵Kses1を有しているため、これらの処理が不要なくなる。

【0251】共通鍵モジュール122の制御部61は、ステップS411において、暗号処理部63を制御して、受信したデータをセッション鍵Kses1で復号し、ステップS422において、復号したデータをメモリ62の対応する領域に保存して利用する。

【0252】次に、図50のフローチャートを参照して、共通鍵モジュール122が、モジュール間通信用リーダライタ2-13と共有するセッション鍵と、公開鍵モジュール121が、モジュール間通信用リーダライタ2-13と共有するセッション鍵とが異なるが、モジュール間通信用リーダライタ2-13が、共通鍵モジュール

ル 122 が有するセッション鍵を、公開鍵モジュール 121 が有するもう一方のセッション鍵で暗号化し、公開鍵モジュール 121 に供給するようになされている場合におけるモジュール間通信について説明する。

【0253】ステップ S451 乃至ステップ S456 において、図 48 のステップ S411 乃至ステップ S416 と同様の処理が実行される。すなわち、モジュール間リーダライタ 2-13 と、公開鍵モジュール 121 の間で、セッション鍵 Kses1 が共有され、モジュール間リーダライタ 2-13 と、共通鍵モジュール 122 の間で、セッション鍵 Kses2 が共有される。

【0254】ステップ S457 において、モジュール間通信用リーダライタ 2-13 の制御部 101 は、暗号処理部 102 を制御して、セッション鍵 Kses2 を、セッション鍵 Kses1 で暗号化させ、公開鍵モジュール 121 に送信する。公開鍵モジュール 121 の制御部 61 は、暗号処理部 33 の共通鍵処理部 42 を制御して、受信したデータをセッション鍵 Kses1 で復号させることにより、セッション鍵 Kses2 を取り出す。

【0255】ステップ S459 において、図 48 のステップ S417 と同様の処理が実行される。ステップ S460 において、公開鍵モジュール 121 の制御部 61 は、移動するデータをセッション鍵 Kses2 で暗号化し、暗号化データをモジュール間通信用リーダライタ 2-13 に送信する。

【0256】ステップ S461 において、図 49 のステップ S440 と同様の処理が実行される。そして、ステップ S462 およびステップ S463 において、図 48 のステップ S422 および S423 と同様の処理が実行される。

【0257】すなわち、図 48 のステップ S420 およびステップ S421 においては、受信したデータをセッション鍵 Kses1 で復号し、復号したデータをセッション鍵 Kses2 で暗号化した後に共通鍵モジュール 122 に送信したが、ここでは、図 49 を用いて説明した処理と同様に、共通鍵モジュール 122 と、公開鍵モジュール 121 とが、同一のセッション鍵 Kses2 を得ることができ、これらの処理を行う必要がない。

【0258】そして、図 51 のフローチャートを参照して、公開鍵モジュール 121 と共通鍵モジュール 122 が、共通秘密鍵 K_{common} を共有し、それを用いて相互認証を行い、更に、共通のセッション鍵 Kses を共有する場合の、モジュール間通信について説明する。

【0259】ステップ S471 およびステップ S472 において、公開鍵モジュール 121 と共通鍵モジュール 122 は、共通秘密鍵 K_{common} により、相互認証を行い、セッション鍵 Kses を共有する。ステップ S473 において、モジュール間通信用リーダライタ 2-13 は、ステップ S471 およびステップ S472 における相互認証の通信路のみ提供する（すなわち、公開鍵モジュール 121 と共通鍵モジュール 122 とともに、セッション鍵の共有は行われない）。

ル 121 と共通鍵モジュール 122 とともに、セッション鍵の共有は行われない）。

【0260】ステップ S474 において、図 48 のステップ S417 と同様の処理が実行される。ステップ S475 において、公開鍵モジュール 121 の制御部 61 は、暗号処理部 33 の共通鍵処理部 42 を制御して、移動するデータをセッション鍵 Kses で暗号化させ、暗号化データをモジュール間通信用リーダライタ 2-13 に送信する。そして、ステップ S476 乃至ステップ S478 において、図 49 のステップ S421 乃至ステップ S423 と同様の処理が実行される。

【0261】すなわち、図 51 を用いて説明したモジュール間通信においては、モジュール間通信用リーダライタ 2-13 は、データの通信路を提供するのみで、モジュール間通信されるデータを暗号化したり、復号することはない。

【0262】上述した一連の処理は、ソフトウェアにより実行することもできる。そのソフトウェアは、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、記録媒体からインストールされる。

【0263】この記録媒体は、図 9 に示すように、コンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク 115（フロッピー（登録商標）ディスクを含む）、光ディスク 116（CD-ROM（Compact Disk-Read Only Memory）、DVD（Digital Versatile Disk）を含む）、光磁気ディスク 117（MD（Mini-Disk）を含む）、もしくは半導体メモリ 118 などよりなるパッケージメディアなどにより構成される。

【0264】また、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0265】

【発明の効果】本発明のデータ記憶装置、データ記憶方法、および記録媒体に記録されているプログラムによれば、情報処理装置に対するデータの入出力を制御し、複数のサービスに対応するデータの記憶を制御し、複数のサービスのうちの第 1 のサービスに対応する第 1 のサービス ID と、入出力制御ステップの処理により第 1 のサービスに関するデータの入出力が制御されている場合にデータの入出力が許可される、複数のサービスのうちの第 2 のサービスに対応する第 2 のサービス ID の記憶を制御するようにしたので、所定のサービスに関するデータの授受を実行している場合において、セキュリティを確保しつつ、予め許可された他のサービスに関するデータ

タの授受を、並行して行うことを可能とすることができる。

【図面の簡単な説明】

【図1】ICカードとリーダライタの通信方式および認証方式について説明するための図である。

【図2】カード発行者、サービス提供者、およびカード保持者の関係について説明するための図である。

【図3】ICカードの構成を示すブロック図である。

【図4】ICカードの構成を示すブロック図である。

【図5】図3および図4の暗号処理部について説明するための図である。

【図6】図3および図4のSRAについて説明するための図である。

【図7】図6のSRAに格納される認証鍵情報について説明するための図である。

【図8】図3および図4のSRTについて説明するための図である。

【図9】リーダライタの構成を示すブロック図である。

【図10】サービス登録用リーダライタのメモリ情報を説明するための図である。

【図11】一般リーダライタのメモリ情報を説明するための図である。

【図12】モジュール間通信用リーダライタのメモリ情報を説明するための図である。

【図13】モジュール間通信を説明するための図である。

【図14】バージョンアップ用リーダライタのメモリ情報を説明するための図である。

【図15】ICカードとリーダライタの認証処理について説明するためのフローチャートである。

【図16】リーダライタのサービス識別処理について説明するためのフローチャートである。

【図17】ICカードのサービス識別処理について説明するためのフローチャートである。

【図18】リーダライタのサービス識別処理について説明するためのフローチャートである。

【図19】ICカードのサービス識別処理について説明するためのフローチャートである。

【図20】リーダライタの認証鍵識別処理について説明するためのフローチャートである。

【図21】ICカードの認証鍵識別処理について説明するためのフローチャートである。

【図22】リーダライタの認証鍵識別処理について説明するためのフローチャートである。

【図23】ICカードの認証鍵識別処理について説明するためのフローチャートである。

【図24】証明書について説明するための図である。

【図25】署名生成処理について説明するためのフローチャートである。

【図26】署名検証処理について説明するためのフロー

チャートである。

【図27】リーダライタの認証鍵識別処理について説明するためのフローチャートである。

【図28】ICカードの認証鍵識別処理について説明するためのフローチャートである。

【図29】サービス登録用リーダライタのサービス登録処理について説明するためのフローチャートである。

【図30】ICカードのサービス登録処理について説明するためのフローチャートである。

【図31】サービス登録用リーダライタのサービス削除処理について説明するためのフローチャートである。

【図32】ICカードのサービス削除処理について説明するためのフローチャートである。

【図33】一般リーダライタのサービス削除処理について説明するためのフローチャートである。

【図34】ICカードのサービス削除処理について説明するためのフローチャートである。

【図35】一般リーダライタのサービスデータ取得処理について説明するためのフローチャートである。

【図36】ICカードのサービスデータ送信処理について説明するためのフローチャートである。

【図37】一般リーダライタのサービスデータ取得処理について説明するためのフローチャートである。

【図38】ICカードのサービスデータ送信処理について説明するためのフローチャートである。

【図39】一般リーダライタのサービスデータ書き込み処理について説明するためのフローチャートである。

【図40】ICカードのサービスデータ書き込み処理について説明するためのフローチャートである。

【図41】一般リーダライタのサービスデータ書き込み処理について説明するためのフローチャートである。

【図42】ICカードのサービスデータ書き込み処理について説明するためのフローチャートである。

【図43】バージョンアップ用リーダライタの鍵バージョンアップ処理について説明するためのフローチャートである。

【図44】ICカードの鍵バージョンアップ処理について説明するためのフローチャートである。

【図45】一般リーダライタの鍵バージョンアップ処理について説明するためのフローチャートである。

【図46】ICカードの鍵バージョンアップ処理について説明するためのフローチャートである。

【図47】ICカードの鍵バージョンアップ処理について説明するためのフローチャートである。

【図48】モジュール間通信処理について説明するためのフローチャートである。

【図49】モジュール間通信処理について説明するためのフローチャートである。

【図50】モジュール間通信処理について説明するためのフローチャートである。

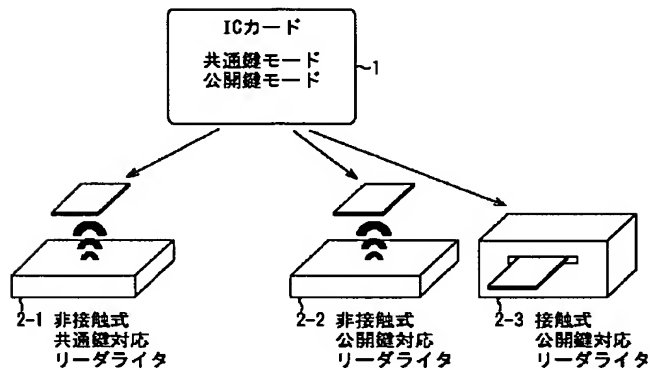
【図51】モジュール間通信処理について説明するためのフローチャートである。

【符号の説明】

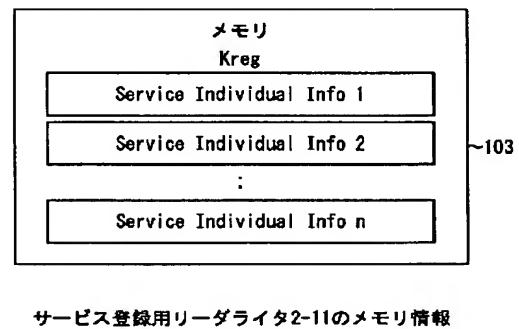
1 ICカード1 リーダライタ、21 通信部、31 制御部、32メモリ、33 暗号処理部、41 公開鍵処理部、42 共通鍵処理部、43 その他の暗号処理部、45 SRT、46 SRA、51 通信部、52 共通鍵サービス処理部、*

* 53 通信部、54 公開鍵サービス処理部、61 制御部、62 メモリ、63 暗号処理部、91 通信部、101 制御部、102 暗号処理部、103 メモリ、111公開鍵処理部、112 共通鍵処理部、113 その他の暗号処理部、105 表示部、106 入力部、121 公開鍵モジュール、122 共通鍵モジュール

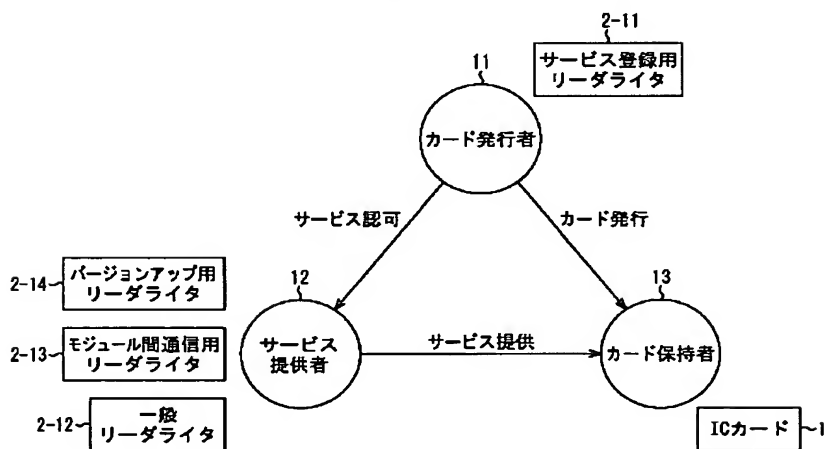
【図1】



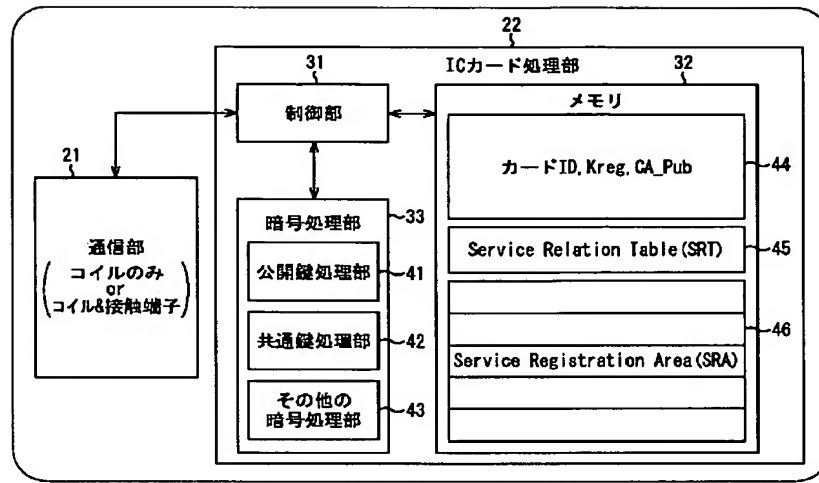
【図10】



【図2】

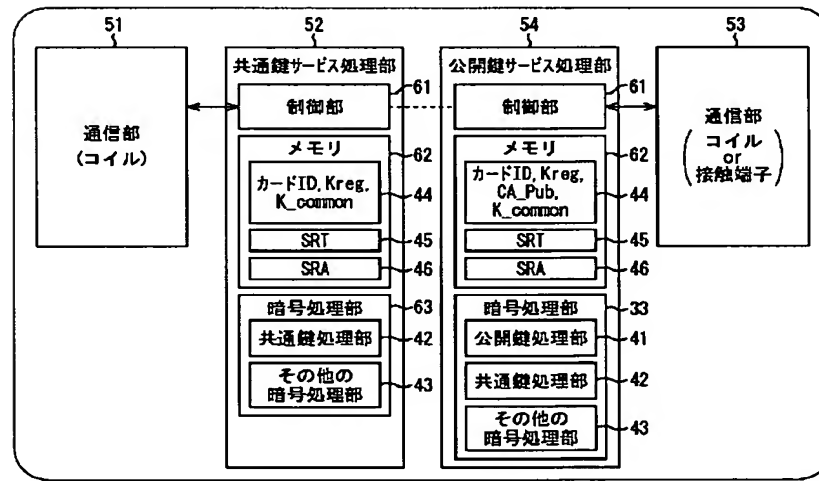


【図3】



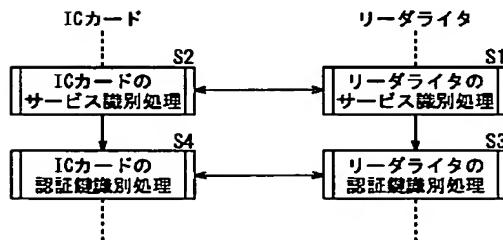
ICカード 1

【図4】

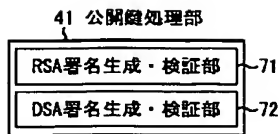


ICカード 1

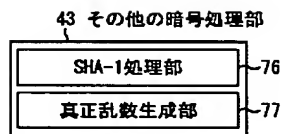
【図15】



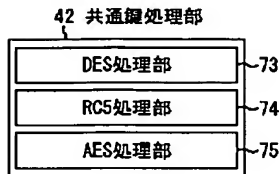
【図5】



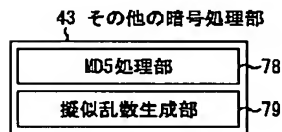
(A)



(C)

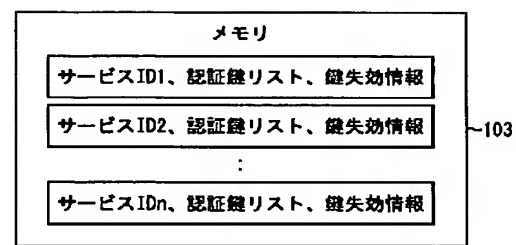


(B)



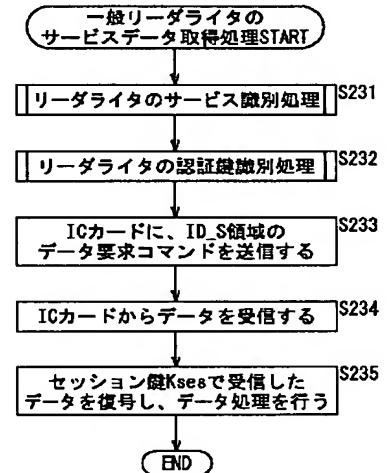
(D)

【図11】

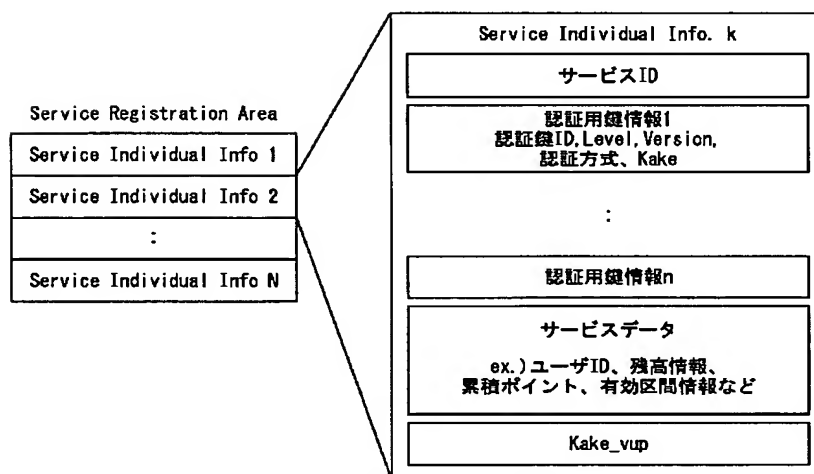


一般リーダライタ2-12のメモリ情報

【図35】

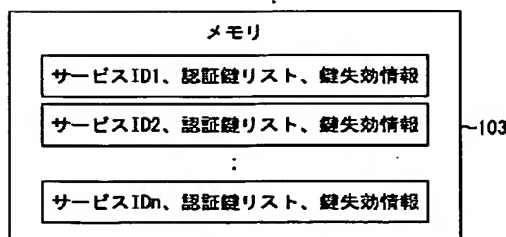


【図6】



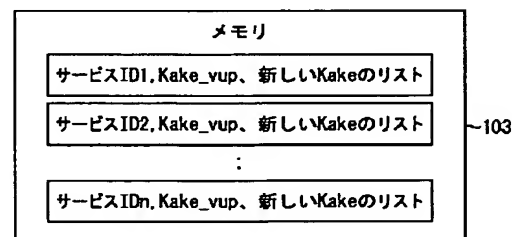
SRAに格納されている情報

【図12】



モジュール間通信用リーダライタ 2-13のメモリ情報

【図14】



バージョンアップ用リーダライタ 2-14のメモリ情報

【図7】

共通鍵・公開鍵の2種類の登録格納状態

領域No.	登録ID	Version	登録方式	Key	Certificate
1	0005	3	共、DES56bit	0100...01	None
2	0018	2	公、ECG128bit	0110...11	証明書データ

(A)

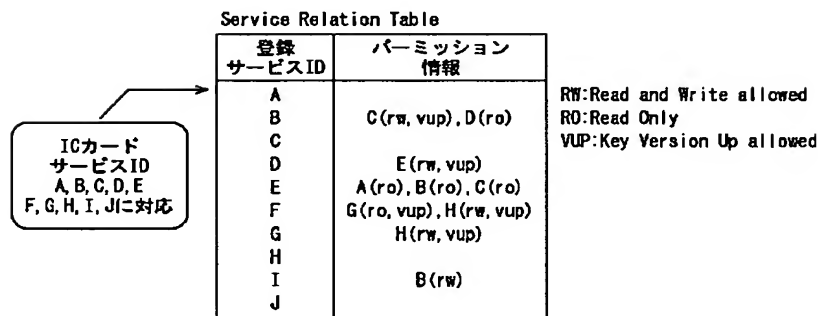
複数レベルの格納状態

領域No.	登録ID	Level	Version	登録方式	Key	Certificate
1	0005	1	3	共、DES56bit	0100...01	None
2	0018	5	2	共、AES128bit	0110...11	None
3	0434	3	1	公、RSA512bit	0011...10	証明書データ
4	0124	6	6	公、RSA2048bit	1011...01	証明書データ
5	0855	2	4	共、AES256bit	1001...00	None
6	0435	4	1	公、ECG160bit	1110...11	証明書データ
7	0342	7	1	公、ECG224bit	0101...10	証明書データ

(B)

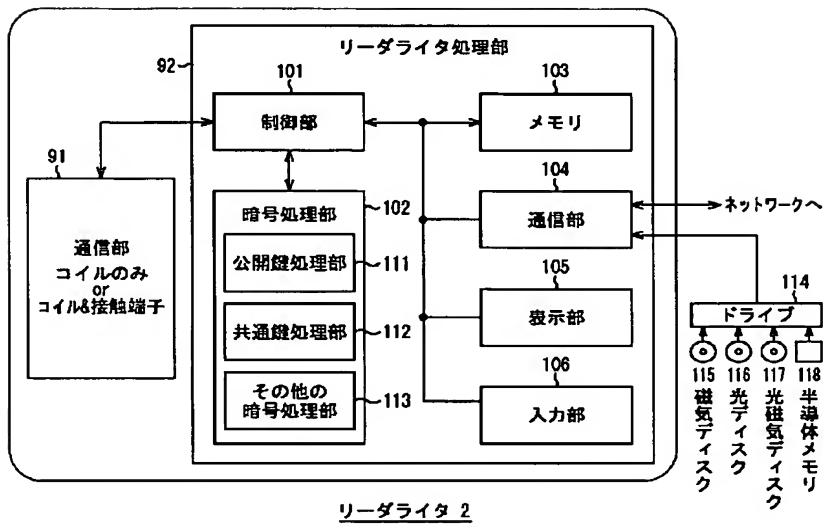
登録用鍵情報

【図8】

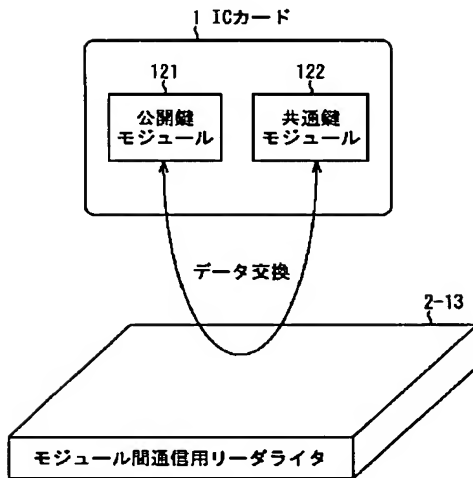


Service Relation Tableに格納されている情報

【図9】

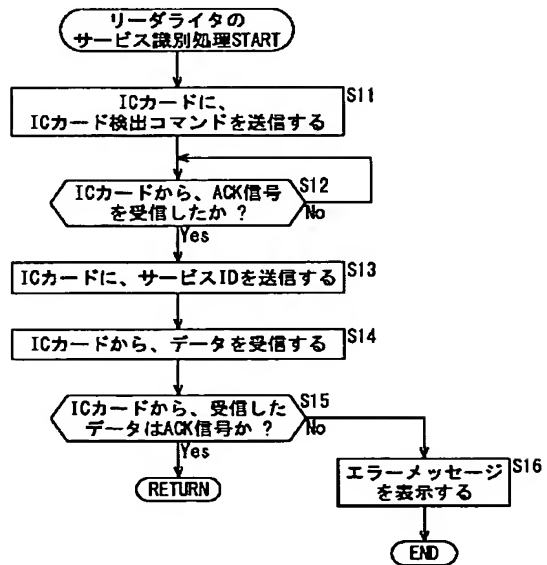


【図13】

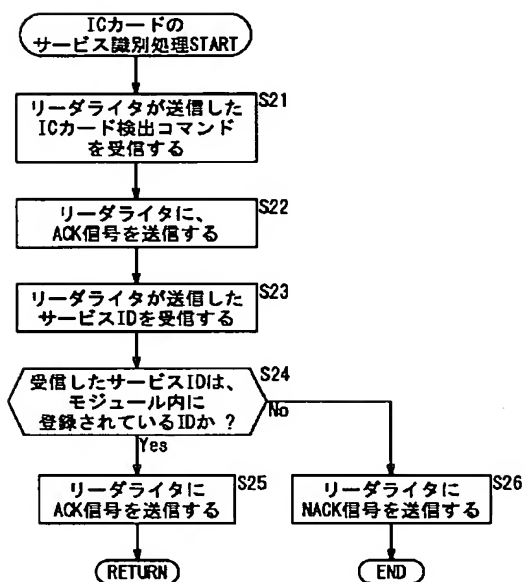


モジュール間通信

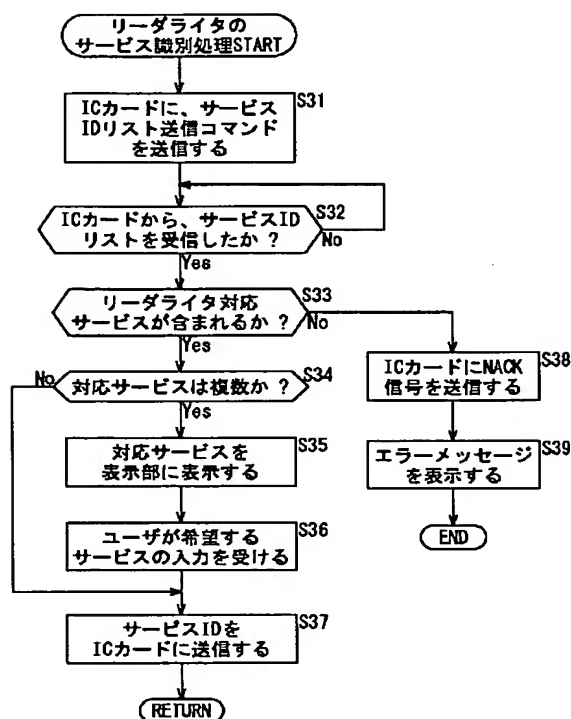
【図16】



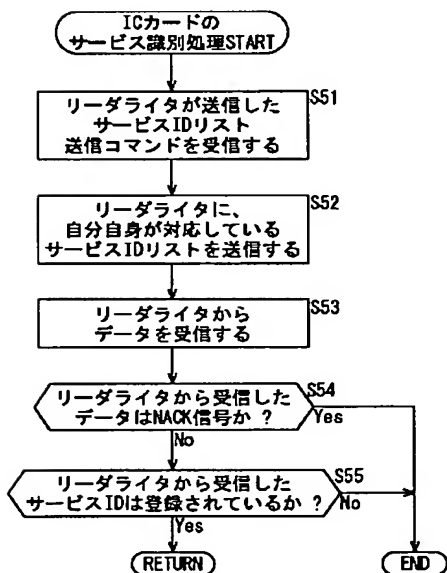
【図17】



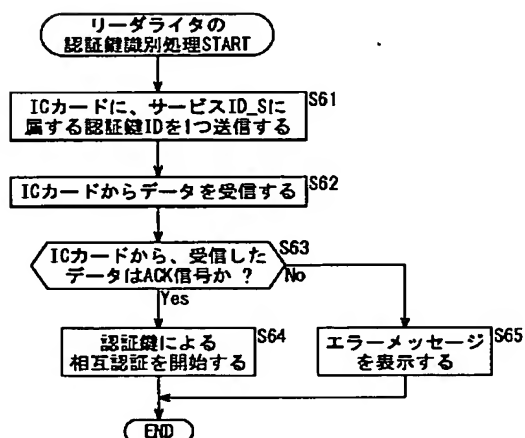
【図18】



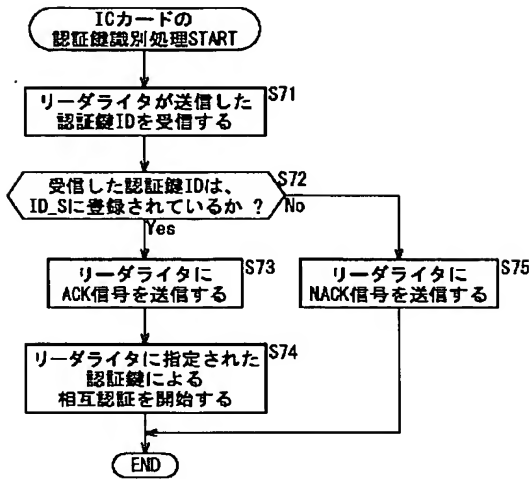
【図19】



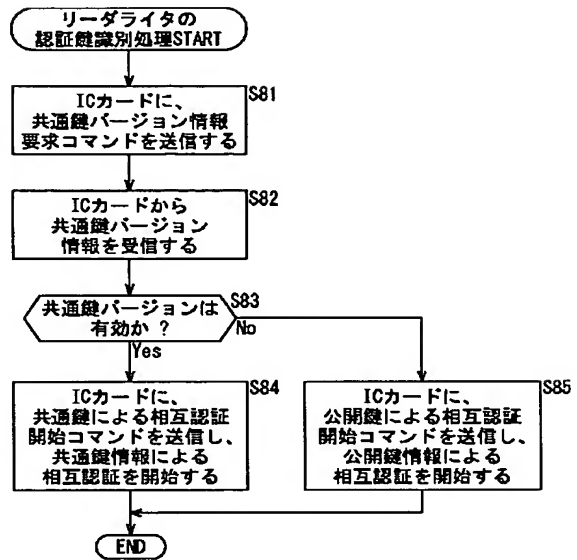
【図20】



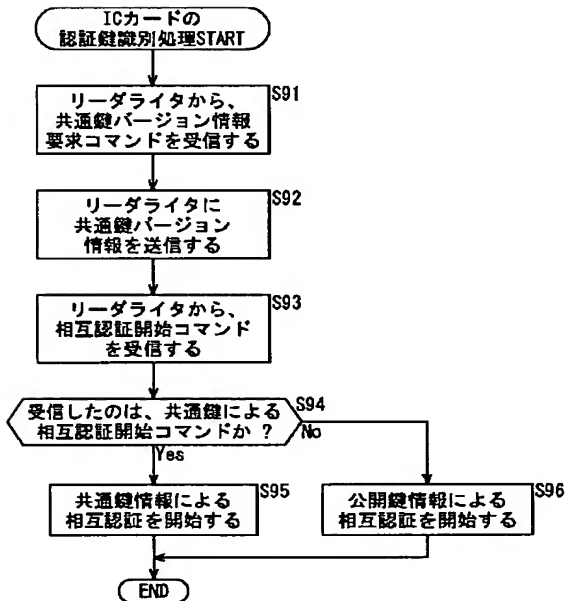
【図21】



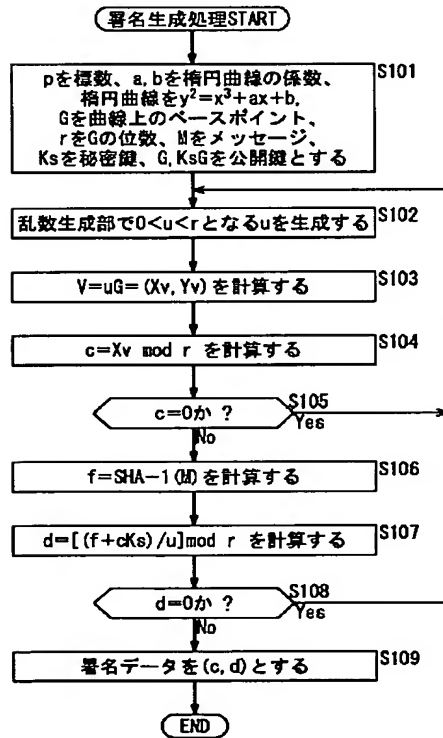
【図22】



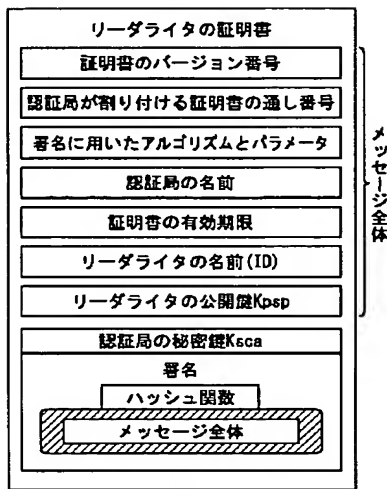
【図23】



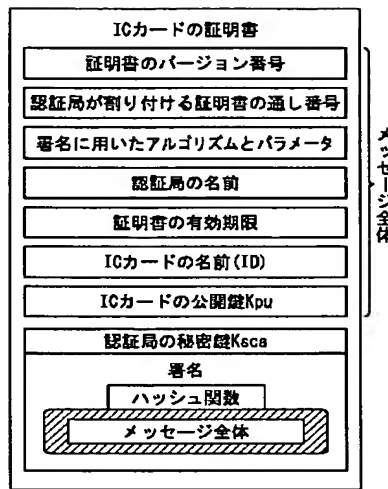
【図25】



【図24】

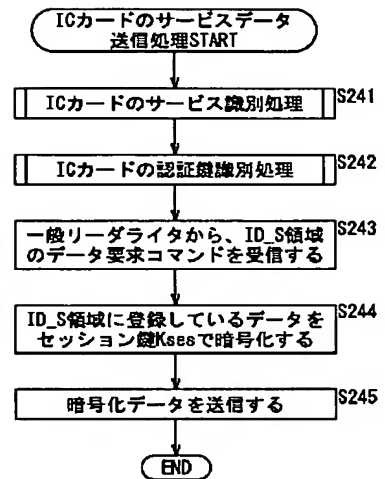


(A)

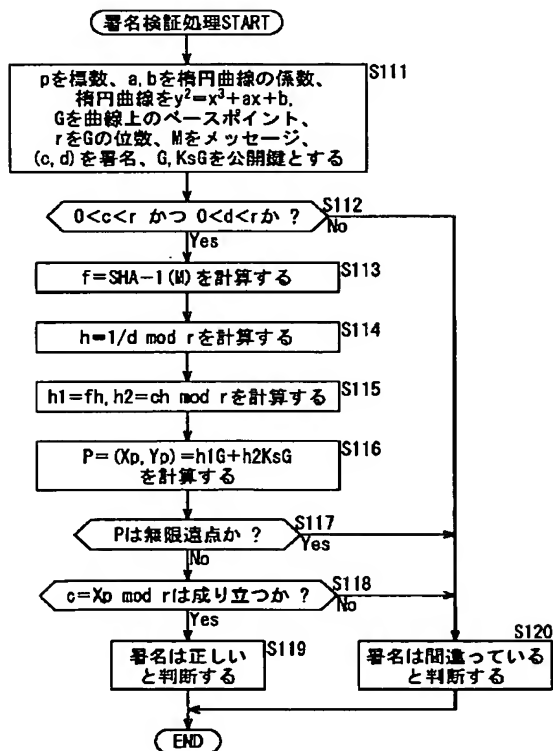


(B)

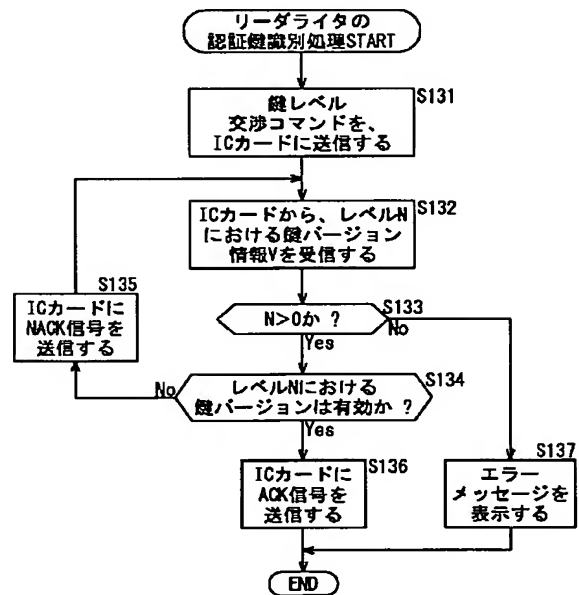
【図36】



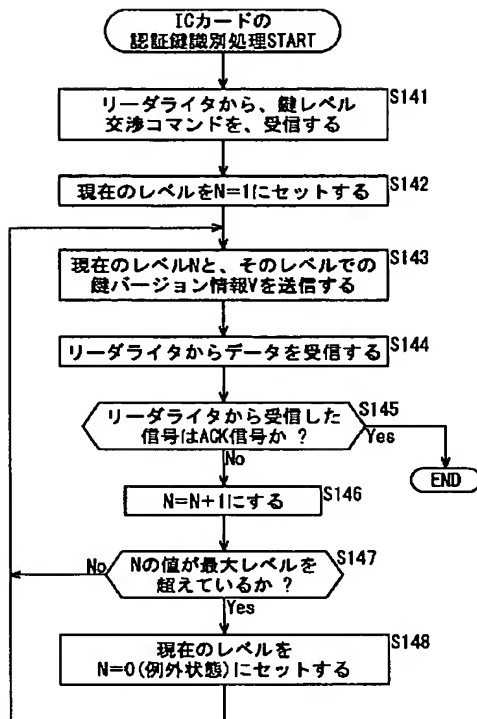
【図26】



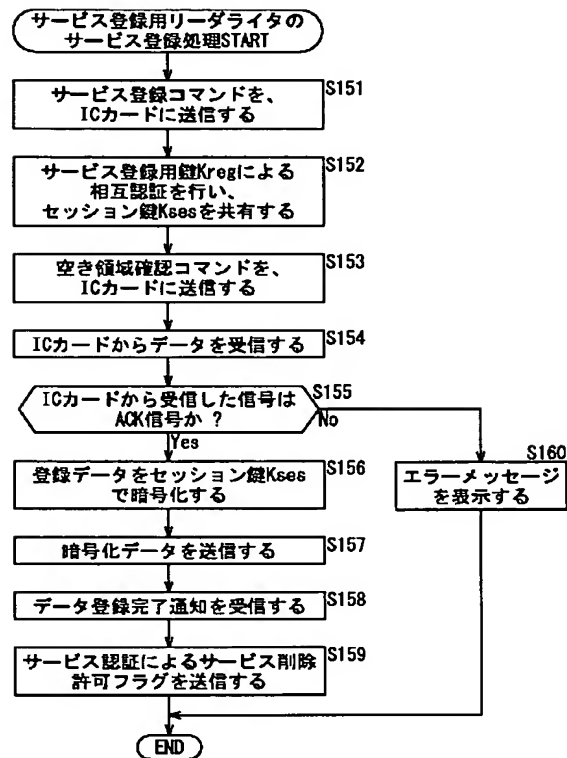
【図27】



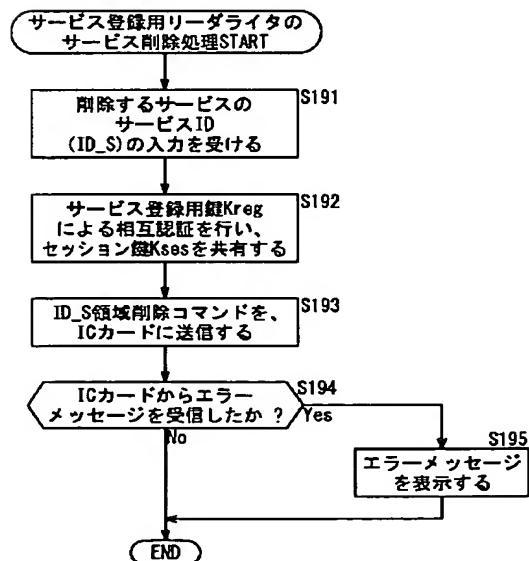
【図28】



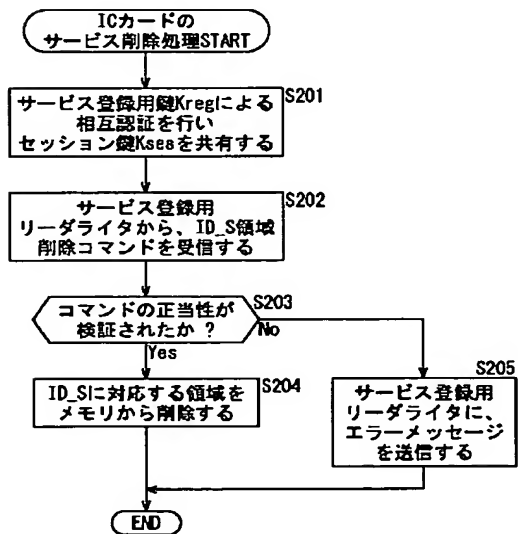
【図29】



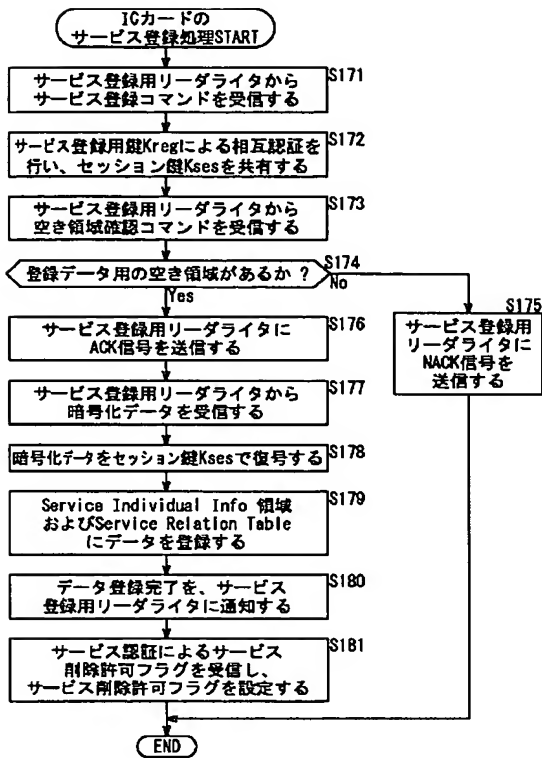
【図31】



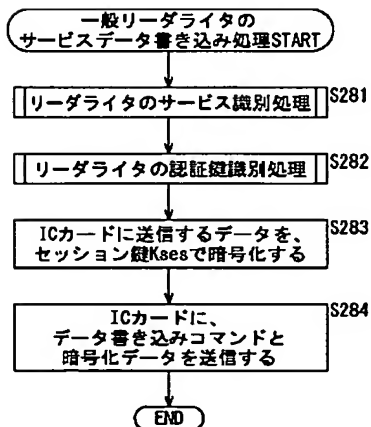
【図32】



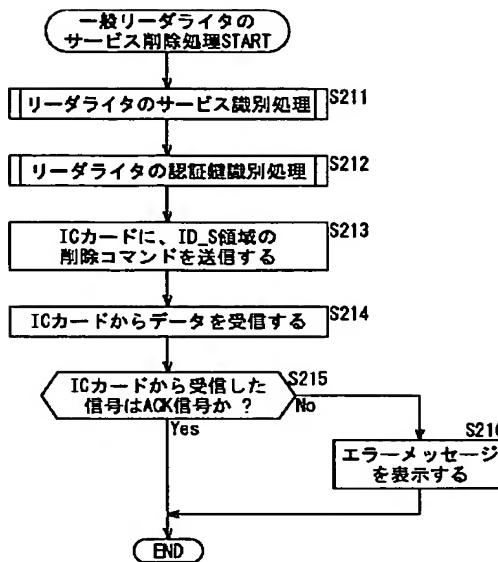
【図30】



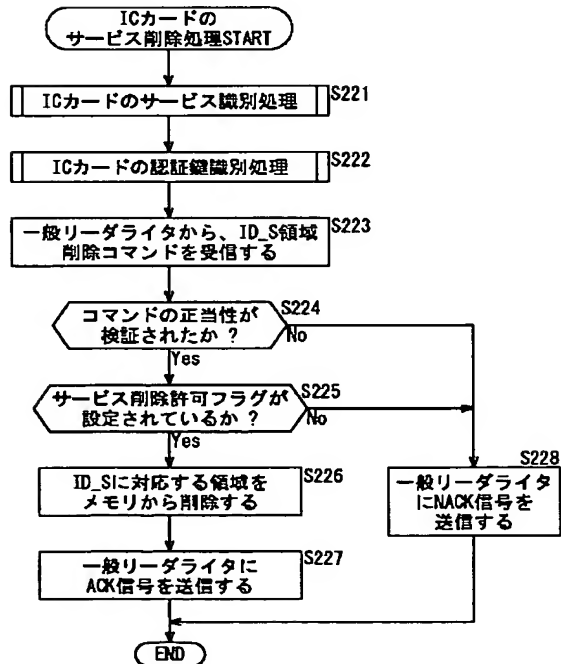
【図39】



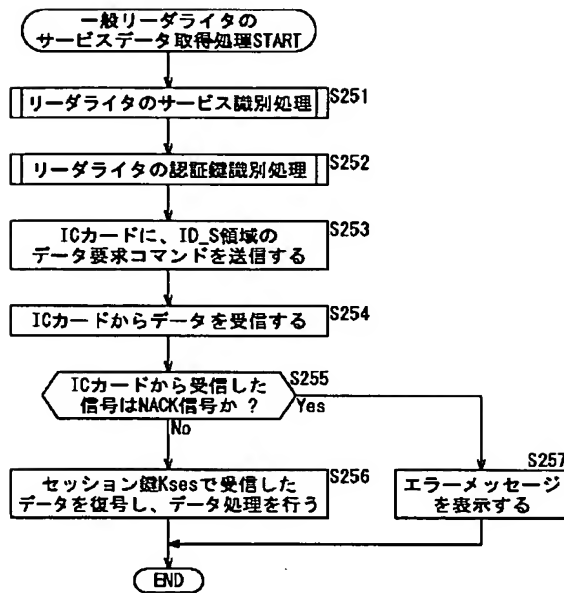
【図33】



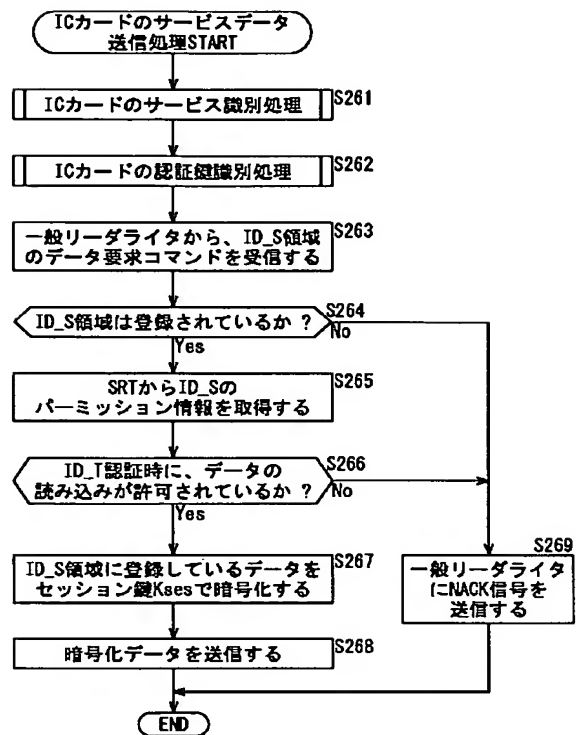
【図34】



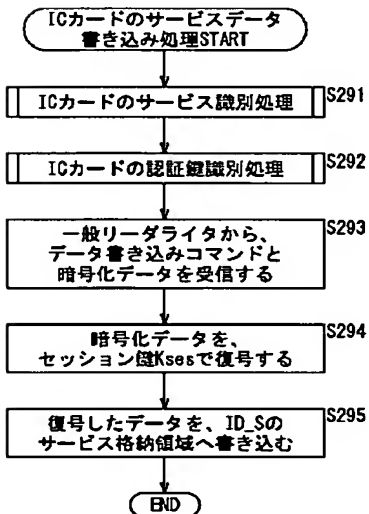
【図37】



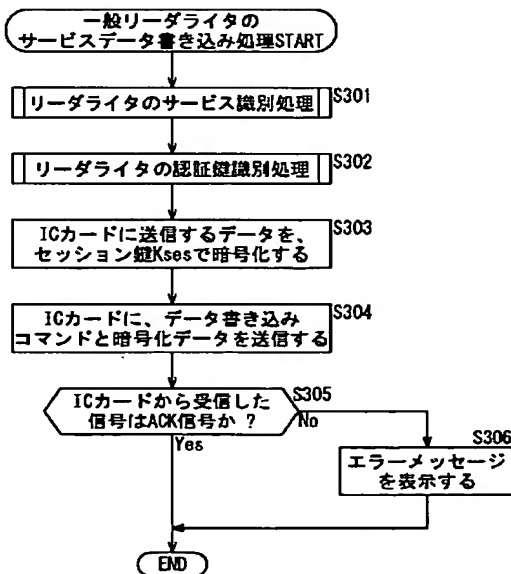
【図38】



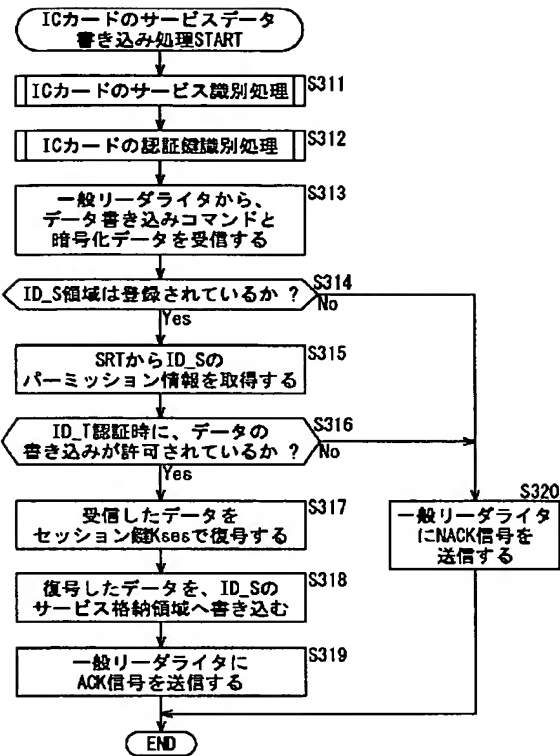
【図40】



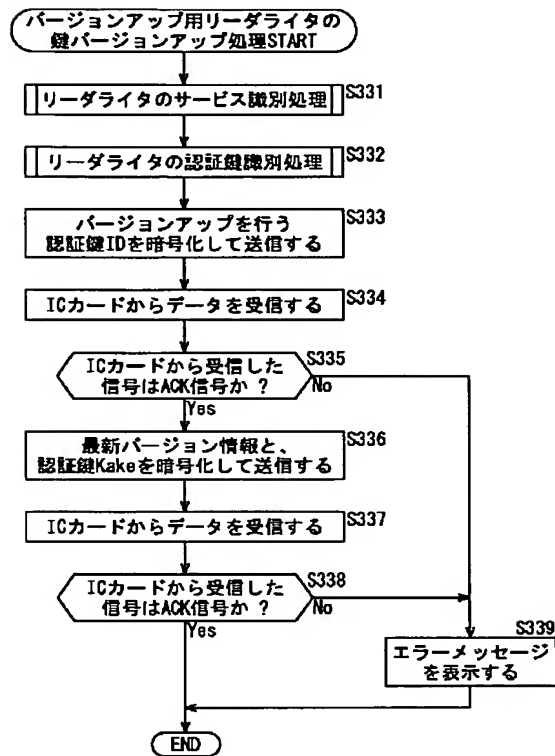
【図41】



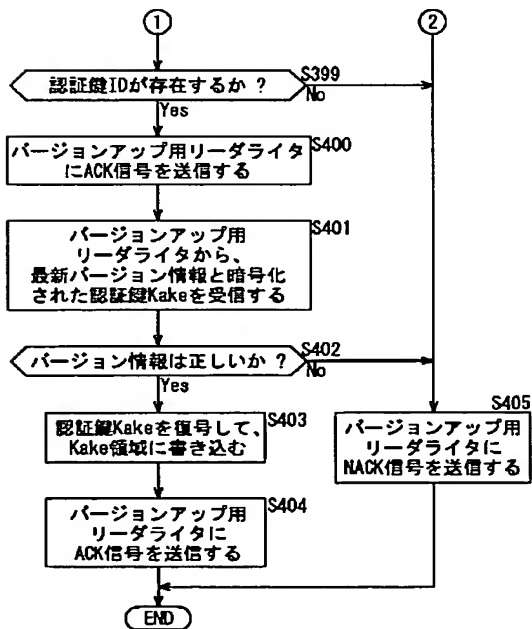
【図42】



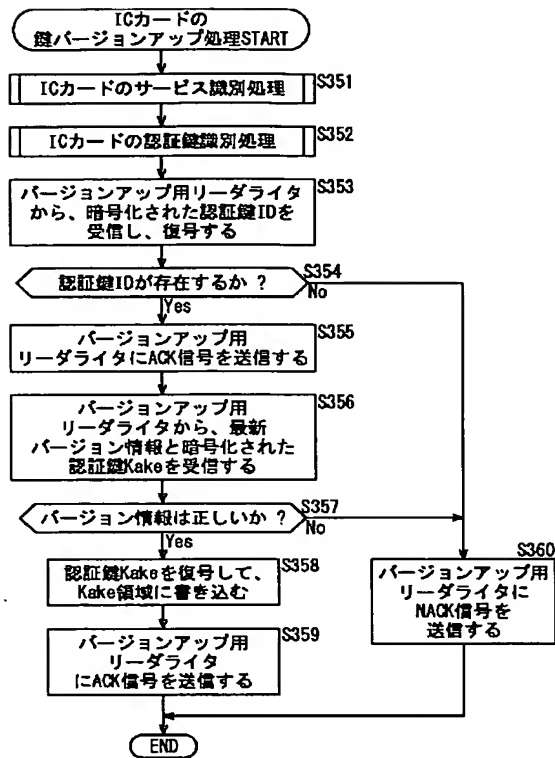
【図43】



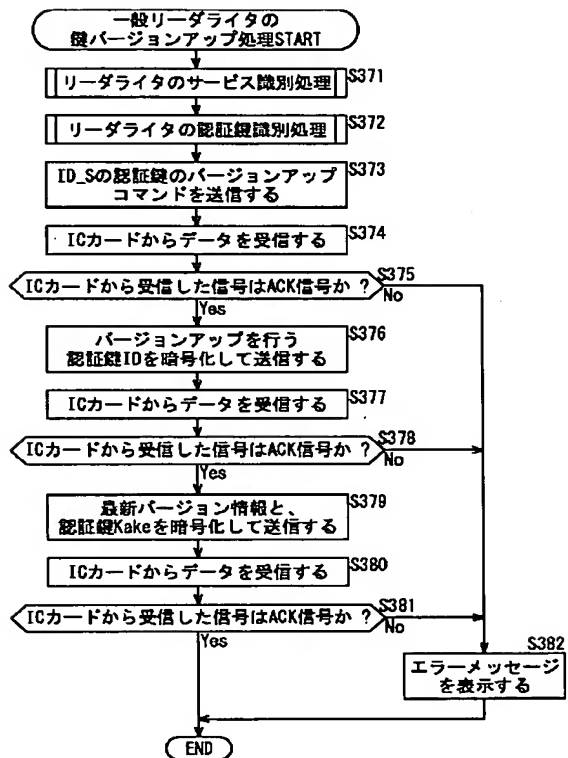
【図47】



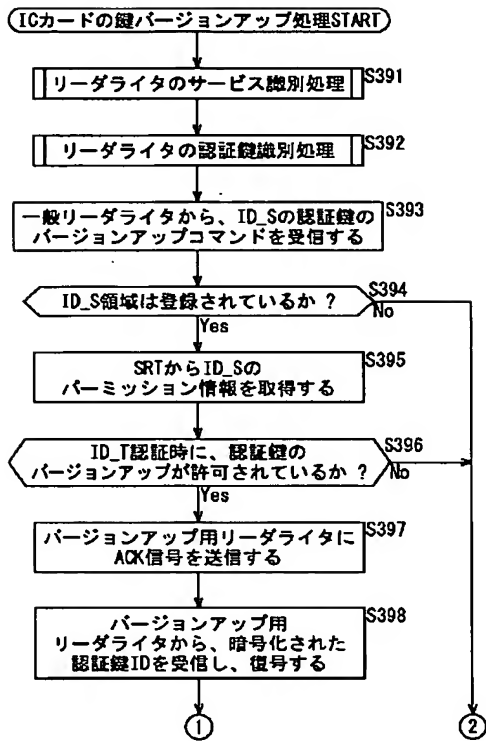
【図44】



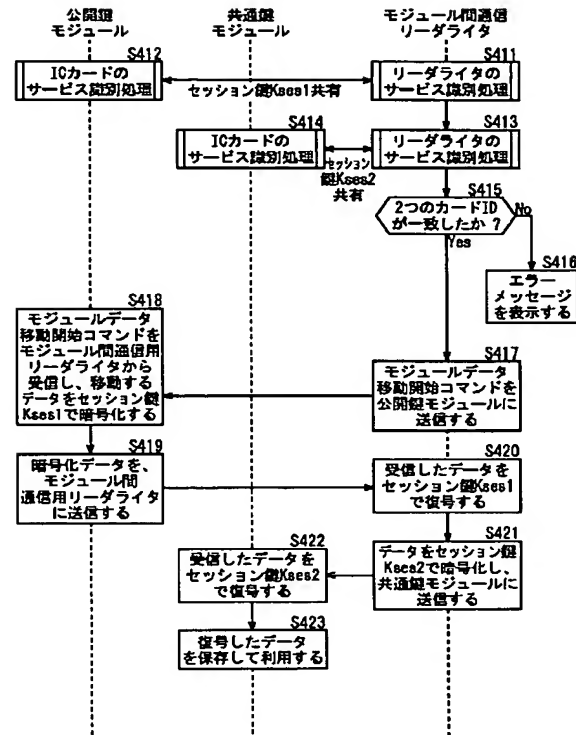
【図45】



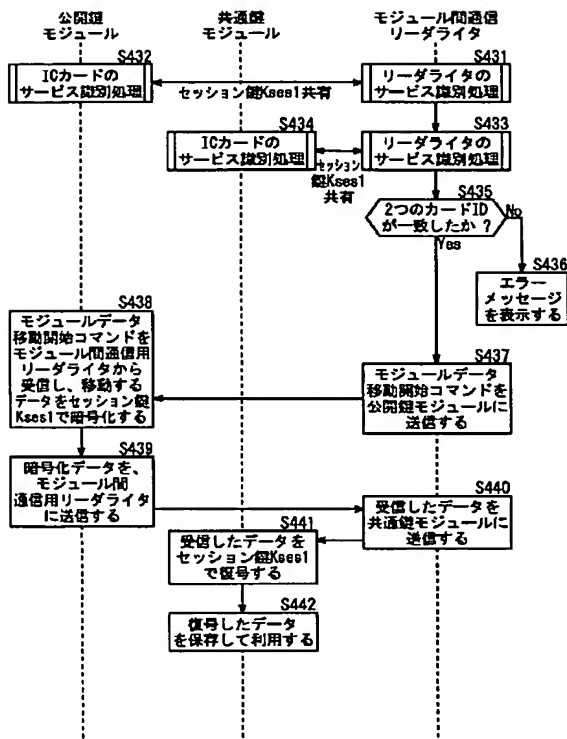
【図46】



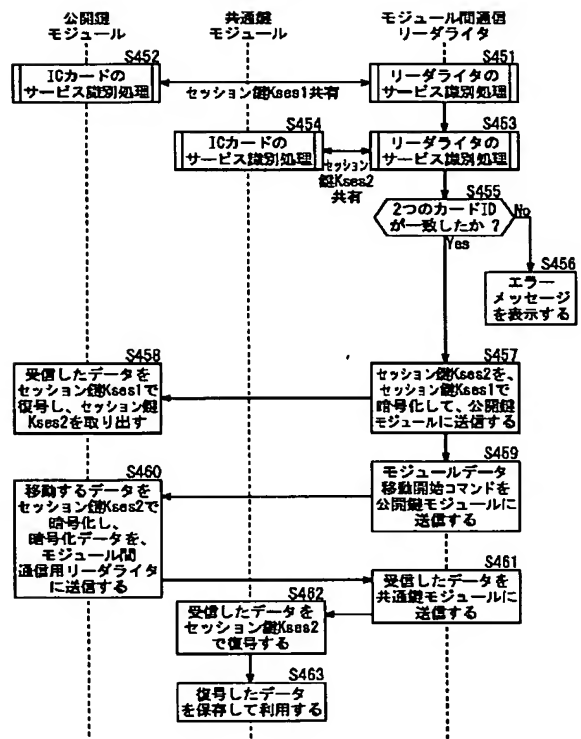
【図48】



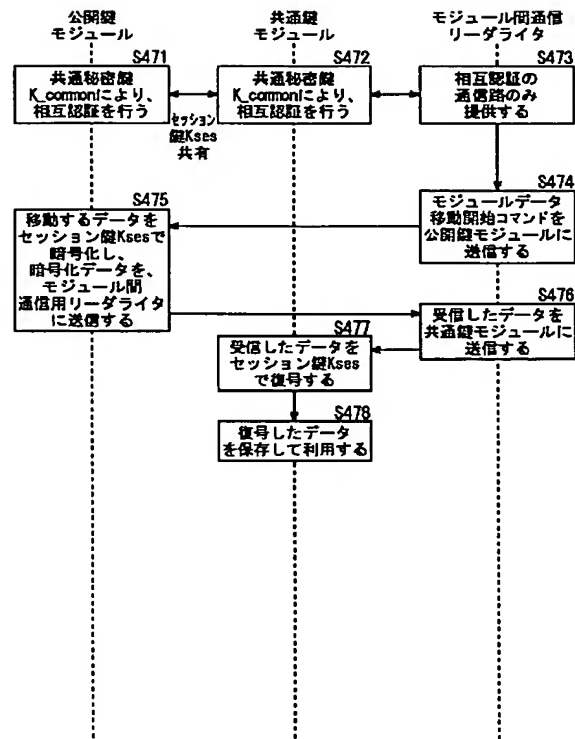
【図49】



【図50】



【図51】



フロントページの続き

(72)発明者 浅野 智之
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内
(72)発明者 吉野 賢治
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(72)発明者 岡 誠
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内
(72)発明者 瀧 隆太
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

Fターム(参考) 5B035 AA13 BB09 BC02 CA23
5B058 CA15 KA11 KA33 KA35 YA06
5J104 AA07 KA01 NA35 NA36 NA38
NA41